# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EXECUTIVE SUMMARY</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>REGULATORY ENVIRONMENT FOR INNOVATION</strong></td>
<td>4</td>
</tr>
<tr>
<td>Who are the relevant regulators in the region?</td>
<td>4</td>
</tr>
<tr>
<td>What are the types of fintech/insurtech activities that are regulated?</td>
<td>9</td>
</tr>
<tr>
<td>What is the attitude and what are the policy views of the regulator in</td>
<td>17</td>
</tr>
<tr>
<td>relation to insurtech (if any)? Is innovation encouraged?</td>
<td></td>
</tr>
<tr>
<td>What are the licenses required and what are the criteria and process</td>
<td>25</td>
</tr>
<tr>
<td>involved?</td>
<td></td>
</tr>
<tr>
<td>Is the use of telematics and/or biometrics regulated?</td>
<td>36</td>
</tr>
<tr>
<td>Does the regulator draw a distinction between institutions that are</td>
<td>39</td>
</tr>
<tr>
<td>&quot;too big to fail&quot; versus &quot;too small to care&quot;?</td>
<td></td>
</tr>
<tr>
<td><strong>TECHNOLOGY AND RISK MANAGEMENT</strong></td>
<td>42</td>
</tr>
<tr>
<td>What laws (if any) do insurance companies have to comply with in</td>
<td>42</td>
</tr>
<tr>
<td>respect of technology risk management?</td>
<td></td>
</tr>
<tr>
<td><strong>DATA PRIVACY</strong></td>
<td>46</td>
</tr>
<tr>
<td>Are there any laws governing big data, including the collection, use,</td>
<td>46</td>
</tr>
<tr>
<td>storage, disclosure and transfer of personal data?</td>
<td></td>
</tr>
<tr>
<td>Are there any restrictions that could hinder the growth and usage of</td>
<td>54</td>
</tr>
<tr>
<td>insurtech by insurance companies under data privacy laws?</td>
<td></td>
</tr>
<tr>
<td><strong>CYBERSECURITY</strong></td>
<td>58</td>
</tr>
<tr>
<td>Are there any laws governing cybersecurity or to mitigate cybersecurity</td>
<td>58</td>
</tr>
<tr>
<td>concerns?</td>
<td></td>
</tr>
<tr>
<td><strong>MARKET TRENDS</strong></td>
<td>63</td>
</tr>
<tr>
<td>What innovations are insurance companies and/or regulators looking at</td>
<td>63</td>
</tr>
<tr>
<td>implementing?</td>
<td></td>
</tr>
<tr>
<td>Have there been fintech/insurtech-related cases (including competition</td>
<td>66</td>
</tr>
<tr>
<td>and/or data privacy) in Asia Pacific?</td>
<td></td>
</tr>
<tr>
<td>What are the most immediate challenges to insurtech innovation?</td>
<td>68</td>
</tr>
<tr>
<td>What has been, or could be, the impact of fintech/insurtech on the</td>
<td>72</td>
</tr>
<tr>
<td>financial services industry?</td>
<td></td>
</tr>
<tr>
<td>What insurtech trends or disruptions may impact insurance companies?</td>
<td>74</td>
</tr>
<tr>
<td><strong>ASIA PACIFIC INSURANCE TEAM</strong></td>
<td>78</td>
</tr>
</tbody>
</table>
Insurtech, one of the buzzwords in disruptive technology, is the latest wave of digital innovation that seeks to displace existing market practices and products in the insurance industry in a way that will bring its customers more convenience, cost-efficiency and effectiveness.

Although insurtech in Asia Pacific is still in its infancy stage, the past few years have witnessed the sector grow at an exponential rate, attracting venture capital investors from all across the globe. While it might to be too early to herald insurtech’s success, one thing is for certain: insurtech is here to stay.

In the same vein, the regulatory regime across multiple jurisdictions have had to evolve so as to ensure that fintech and insurtech innovations will not be stymied by overly complex rules and regulations. The *Asia Pacific Guide for Insurtech Innovation and Utilization* provides a high-level comparative overview of the market trends and latest applicable laws in 12 jurisdictions, in respect of concerns that may arise in the development and utilization of insurtech.
The Australian Securities and Investments Commission's (ASIC) and the Australian Prudential Regulation Authority (APRA) are the two main regulators for the fintech/insurtech industry.

ASIC is Australia’s corporate, markets and financial services regulator. In particular, ASIC’s Innovation Hub provides informal guidance and support to eligible start-ups, which helps fintech/insurtech entrants minimize the time and cost required to navigate the regulatory landscape.

Further, ASIC meets regularly with international regulators, including the Financial Conduct Authority in the United Kingdom and European Securities and Markets Authority, to discuss partnerships opportunities, innovation developments and policy proposals.

The Australian Prudential Regulation Authority (APRA) is another regulator of the Australian financial services industry. It is responsible for regulating authorized deposit-taking institutions (such as banks), insurance companies and other financial institutions it supervises. APRA is actively looking to reduce barriers for new entrants into the banking and insurance sectors.

The Australian Competition and Consumer Commission (ACCC) is Australia’s competition regular and, among other things, helps maintain competition in the financial system by ensuring the viability of emerging fintech/insurtech entrants.

The Office of the Australian Information Commissioner regulates data privacy matters.

Although fintech and insurtech are not terminologies recognized by the Chinese government or used in published laws and regulations, according to the Guidelines on the Promotion of the Healthy Development of Internet Finance (FinTech Guidelines) issued on 18 July 2015, which is considered to be the first comprehensive regulation concerning regulation of fintech in China, the division of responsibilities between financial regulators is as follows:

- People’s Bank of China is responsible for the regulation and supervision of internet payment services.
- China Securities Regulatory Commission is responsible for the regulation and supervision of (i) internet lending services and (ii) internet trust and internet consumer finance.
- China Securities Regulatory Commission is responsible for the regulation and supervision of (i) equity crowdfunding activities and (ii) internet fund sales.
- China Insurance Regulatory Commission is responsible for the regulation and supervision of internet insurance services.

In July 2017, the Financial Stability and Development Commission was established to be the central regulator to coordinate with these financial regulations in respect of the regulation of financial sectors.

In addition to these financial regulators, the Ministry of Industry and Information Technology (MIIT) is responsible for the regulation and supervision of telecommunications-related businesses involved in the provision of fintech/insurtech, the Cybersecurity Administration of China (CAC) is responsible for the regulation of cybersecurity compliance in the provision of fintech/insurtech and the CAC, together with the Ministry of Public Security (PSB), will regulate compliance with the handling of personal information in the provision of fintech/insurtech.
**HONG KONG**

The Insurance Authority (IA) is Hong Kong’s insurance regulator overseeing the financial conditions and operations of authorized insurers. There are also three self-regulatory bodies overseeing the activities of insurance intermediaries, namely (in relation to insurance agents and agencies) the Hong Kong Federation of Insurers (HKFI); (in relation to insurance brokers) the Hong Kong Confederation of Insurance Brokers (HKCIB) and Professional Insurance Brokers Association (PIBA). However, the supervisory functions of the three self-regulatory bodies will be taken up by the IA (expected to be in 2018 or 2019). If the fintech/insurtech activities involve moneylending, the regulator is the registry of moneylenders, whose function is performed by the Companies Registry.

The Hong Kong Monetary Authority (HKMA) is the banking regulator overseeing institutions such as banks and deposit-taking companies. The Securities and Futures Commission (SFC) is the regulator regulating securities intermediaries such as brokers, investment advisers and fund managers in the securities and futures sectors. The SFC also regulates certain investment products and other listing matters.

The Office of the Privacy Commissioner for Personal Data (PCPD) is the regulator overseeing data privacy matters and enforcing the Personal Data (Privacy) Ordinance (Cap. 486).

The Communications Authority is the body regulating Hong Kong’s broadcasting and telecommunications industries.

The Intellectual Property Department (IPD) is the government department that administers the intellectual property regime.

**INDONESIA**

The main regulator is the Indonesian Financial Services Authority (OJK). The OJK regulates and supervises financial institutions, including insurance companies, and financial service activities in the banking, capital market, insurance and other financial services sectors. Insurtech will be supervised by the OJK.

Bank Indonesia (Indonesia’s central bank) supervises the national payment system and exchange controls (including lending from offshore).

The Capital Investment Coordination Board (BKPM) supervises general foreign investment in Indonesia and to the extent that the OJK does not have jurisdiction, BKPM may have jurisdiction over insurtech depending on actual activities.

The Ministry of Communications and Informatics (MOCI) regulates and supervises telecommunications and media activities in Indonesia. The MOCI will have also a say on the technical aspects of insurtech, including the data protection regime and cybersecurity.

**JAPAN**

The main regulator is the Financial Services Agency (FSA), which is in charge of the supervision of financial institutions, including insurance companies.

Although the Ministry of Economy, Trade and Industry (METI) is not the regulator of the financial sector, it is very supportive of the introduction and promotion of fintech/insurtech-related businesses to the Japanese market and organizes study groups on fintech. See Question 4.
### Malaysia

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>There are several regulators overseeing the financial services sector, and each such regulator would have oversight of their respective regulated institution. Specifically:</td>
</tr>
<tr>
<td></td>
<td>• Bank Negara Malaysia (that is, the Central Bank of Malaysia) (BNM) would have regulatory oversight of fintech-related issues affecting the banking, insurance, money broking, financial advisory, payment systems and instruments, foreign exchange, money-changing and remittance services.</td>
</tr>
<tr>
<td></td>
<td>• Securities Commission Malaysia (SC) would regulate fintech/insurtech activities affecting the capital markets and its participants.</td>
</tr>
</tbody>
</table>

Given that fintech/insurtech involves technology and data, it is likely to also fall within the purview of:

- The Malaysian Communications and Multimedia Commission (MCMC), which regulates the communications and multimedia industry in Malaysia. |
- The Malaysian Personal Data Protection Department (PDPD), which administers the data protection regime. |
- The Intellectual Property Corporation of Malaysia (MyIPO), which administers the intellectual property regime. |

### Myanmar

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The main regulator is the Insurance Business Supervisory Board, which is established under the Ministry of Planning and Finance (MOPF), which currently closely restricts the participants and products in the insurance market within Myanmar. The major market participant, Myanmar Insurance, which was the government monopoly before the market was partially liberalized in 2012, is still required to provide some approvals for market entry as well.</td>
</tr>
<tr>
<td></td>
<td>The Central Bank of Myanmar, which has regulatory oversight of all fintech in Myanmar, is also likely to be a key regulator for the provision or approval.</td>
</tr>
</tbody>
</table>
## Who are the relevant regulators in the region?

<table>
<thead>
<tr>
<th>PHILIPPINES</th>
<th>The relevant regulators are the Securities and Exchange Commission (SEC) (with respect to, among others, capital market participants, financing companies, adjustment companies and lending companies), the Bangko Sentral ng Pilipinas (BSP) or the central bank of the Philippines (with respect to, among others, banks, trust companies and investment management companies), and the Insurance Commission (with respect to insurance companies and insurance intermediaries). Depending on the specific activities involved, other regulators may be involved, including the Department of Trade and Industry, the National Telecommunications Commission (NTC) Office of Cybercrime (OCC), and the National Privacy Commission (NPC). The NTC implements the Public Telecommunications Policy Act of 1995, as amended (Telecoms Law). It also regulates and supervises the provision of public telecommunications services, including value-added services in the telecommunications industry. The 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 (Cybercrime Law). The NPC is the regulatory agency tasked to administer the Philippines' Data Privacy Act of 2012 (DPA). The Intellectual Property Office of the Philippines (IPOPHL) administers the intellectual property regime.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SINGAPORE</td>
<td>The Monetary Authority of Singapore (MAS) is Singapore's central bank and the integrated financial regulator supervising financial institutions in Singapore, including banks, insurance companies, capital markets intermediaries and other financial markets infrastructure. If the fintech/insurtech activities involve moneylending, the regulator is the Registrar of Moneylenders. As a statutory board in the Singapore government, the Infocomm Media Development Authority of Singapore (IMDA) develops and regulates the converged infocomm and media sector, and also seeks to promote and regulate data protection in Singapore through the Personal Data Protection Commission (which is part of the IMDA). The Intellectual Property Office of Singapore (IPOS) administers the intellectual property regime.</td>
</tr>
</tbody>
</table>
| TAIWAN | The Financial Supervisory Commission (FSC) is the competent authority responsible for development, supervision, regulation and examination of financial markets and financial service enterprises in Taiwan. There are four bureaus under the FSC:  
- Banking Bureau  
- Securities and Futures Bureau  
- Insurance Bureau  
- Financial Examination Bureau  
To develop fintech/insurtech in Taiwan, in September 2015, the FSC established the Financial Technology Office (as the coordinator among various bureaus) and the Financial Technology Advisory Committee (as consulting committee). |
### Who are the relevant regulators in the region?

<table>
<thead>
<tr>
<th>Country</th>
<th>Regulations</th>
</tr>
</thead>
</table>
| **THAILAND** | There are several regulators relevant to the operation of fintech/insurtech innovations in Thailand, depending on the operating entities and scope of business activities. Key regulators include the following:  
- Ministry of Finance (MOF) – oversees the operation of financing, securities and credit financier business, and the business of financial institutions in Thailand  
- Bank of Thailand (BOT) – oversees business operation of commercial banks and other financial institutions, including finance companies, ranging from moneylending and currency exchange  
- Securities and Exchange Commission (SEC) – regulator in charge of securities business, including public fundraising through capital market  
- Ministry of Commerce (MOC) – oversees the general business operation of a company incorporated under the laws of Thailand, whether private, public or listed  
- Office of Insurance Commission (OIC) – in charge of business operation of insurance companies in Thailand  
- Electronic Transaction Commission under the Prime Minister – in charge of electronic transaction business conducted in Thailand |
| **VIETNAM**  | There is no single authority that has overall power to regulate fintech/insurtech in Vietnam. In fact, each authority may play a different role in regulating this area:  
- State Bank of Vietnam (SBV) – Vietnam’s central bank takes charge of banking activities (for example, moneylending, payment and settlement systems, money exchange and remittance) and other banking and financial activities of credit institutions.  
- Ministry of Planning and Investment (MPI) is responsible for regulating investment activities (for example, equity crowdfunding platforms).  
- Ministry of Information and Communications (MIC) is responsible for personal data privacy.  
- Ministry of Finance (MOF) is in charge of insurance business by insurers and insurance brokers, as well as securities companies and fund management companies.  
- Ministry of Science and Technology (MOST) is responsible for the intellectual property regime. |
Companies seeking to provide any financial or insurance products or services are required to hold an Australian Financial Services Licence (AFSL) or a credit license. However, ASIC’s regulatory sandbox allows eligible fintech/insurtech businesses to:

- test certain financial and credit services for up to 12 months without needing to apply for a financial services or credit license
- offer products and services to wholesale clients and a limited number of retail clients (up to 100 retail clients only), with appropriate monetary exposure limits in place

The financial or insurance products or services that are exempt under the regulatory sandbox include:

- dealing in all listed or quoted Australian securities
- all deposit products
- debentures, stocks or bonds issued or proposed to be issued by the Australian government
- simple managed investment schemes (that is, a registered scheme that invests at least 80% of its assets in a bank account where funds can be withdrawn within three months, or in arrangements where the investments can be realized at market value within 10 days)
- home contents insurance products
- personal and domestic insurance products

Due to its success, the Australian government is currently looking to enhance these exemptions. The Australian government is looking to:

- extend the testing time frame to 24 months
- allow businesses to test a broader range of financial products and credit services without a license, including providing more holistic financial advice, issuing consumer credit, offering short-term deposit or payment products, and operating a crowdsourced equity funding intermediary

Further, the Australian government has recently proposed the removal of the “double taxation” treatment for goods and services tax (GST) on digital currencies that will help facilitate further developments or use of digital currency.
### CHINA

The following types of activities are currently regulated under the Fintech Guidelines:

- internet payment
- internet lending
- equity crowdfunding
- internet fund sales
- internet insurance
- internet trust and internet consumer finance

In addition, Chinese regulators have been actively clamping down on illegal fundraising through P2P lending and equity crowdfunding.

### HONG KONG

Activities involving authorized insurers, insurance intermediaries and the insurance business may be regulated under the Insurance Ordinance (Cap. 41), Securities and Futures Ordinance (Cap. 571) and their regulations and the relevant guidelines and codes issued by the IA, the SFC, the HKFI, the CIB and PIBA (before the functions of HKFI, CIB and PIBA are taken over by the IA). Authorized insurers seeking to commence or develop insurtech activities must ensure that any new activities comply with the foregoing (as applicable) and do not breach any existing license conditions.

Payment and settlement systems (for example, digital payments) may be regulated under the Payment Systems and Stored Value Facilities Ordinance (Cap. 584), which is administered by the HKMA. Money-changing and remittance businesses will be subject to the requirements of the Money Changers Ordinance (Cap. 34) and the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615).

Virtual currencies (for example, Bitcoin) are not specifically regulated under the Hong Kong regime; however, various financial regulators (for example, HKMA) have reminded financial institutions and intermediaries to maintain an escalated level of vigilance in relation to the money-laundering and terrorist-financing risks associated with virtual commodities.

Any insurtech activities involving offer of investments or securities (for example, equity crowdfunding platforms), the dealing of securities, asset management, securities margin financing, leveraged foreign exchange trading, dealing in futures contracts and other similar activities will potentially be regulated under the Securities and Futures Ordinance (Cap. 571) and the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32).

Insurtech activities involving moneylending may also be regulated under the Money Lenders Ordinance (Cap. 163).

Separately, in relation to cryptography and data encryption products, they may be subject to strategic trade control under the Import and Export Ordinance (Cap. 60) and the Import and Export (Strategic Commodities) Regulations (Cap. 60G). It is possible that a license will need to be obtained for the import/export of such goods. The strategic trade control system in Hong Kong is made up of a licensing system administered by the Trade and Industry Department and an enforcement system under the purview of the Customs and Excise Department.
**What are the types of fintech/insurtech activities that are regulated?**

**INDONESIA**

In brief, there is no specific regulation for insurtech activities, which is a relatively new concept in Indonesia. Although there are no specific fintech/insurtech regulations, the government is aware of technological developments and is now encouraging fintech/insurtech activities. Current laws and regulations impacting on fintech/insurtech activities include the following:

- Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) and its implementing regulation, Government Regulation No. 82 of 2012 on Implementation of Electronic Systems and Transactions (GR 82), which acknowledge electronic contracts such as e-policies. Under the EIT Law, an "electronic system operator" is defined as any person, state entity, business entity and community that provides, manages and/or operates an electronic system whether independently or collectively to an electronic system user for its own use and/or another party's use. Based on the above definitions (which are broad in nature), any person or entity that manages and operates electronic systems, and provides those systems to other parties, will be considered as an electronic system operator.

- OJK Regulation No.1/POJK.07/2013 on Protection for Consumers of Financial Services Sector (POJK 1) and OJK Circular Letter No.13/SEOJK.07/2014 on Standard Agreements, which specifically acknowledges policies in electronic form

- GR 82, which requires all Electronic System Operators for "public service" to have a data center and disaster recovery center onshore by October 2017

- Bank Indonesia Regulation No. 9/15/PBI/2007 (BI Regulation 9/2007) requires the data centers and disaster recovery centers for banks to be located onshore

### JAPAN

Activities related to insurance business may be regulated under the Insurance Business Act and the relevant subordinated regulations and guidelines. The Act on the Protection of Personal Information (APPI) as well as the relevant subordinated regulations and guidelines is also highly relevant as many new insurance products and services related to fintech/insurtech are likely developed through personal information.

Businesses related to payment, fund transfer, settlement and moneylending are subject to the Banking Act, the Money Lending Business Act, the Act for Regulation, etc., of Receiving of Capital Subscription, Deposits, Interest on Deposits, etc., the Payment Services Act, the Installment Sales Act, the Foreign Exchange and Foreign Trade Act and the Act on Prevention of Transfer of Criminal Proceeds (Japanese primary regulations for KYC and AML) as well as their respective subordinate regulations.

Businesses related to investment advisory and investment management would be subject to the Financial Instruments and Exchange Act (FIEA) as well as the subordinate regulations.

The draft amendments to the various financial regulations such as the Banking Act and the Money Lending Business Act, as well as the amendments to the Payment Services Act with the aim of regulating virtual currency exchange businesses, were submitted to the Diet on 4 March 2016 and were passed on 25 May 2016. The amended regulations together with the relevant subordinated regulations came into effect on 1 April 2017.

The draft amendments to the Banking Act, with the aim of regulating electronic collection agency businesses, were submitted to the Diet on 3 March 2017 and were passed on 26 May 2017.

The introduction of fintech/insurtech to the Japanese financial market seems to be still at an early stage and a desirable regulatory framework on fintech/insurtech is still under study and discussion by the regulator and market players, although many regulations related to fintech/insurtech have been recently introduced (please see 4 below). Further regulatory amendments, with the aim of covering the cross-sectoral and cross-border development of fintech/insurtech, may therefore be promoted and implemented.

### MALAYSIA

Activities involving insurance, banking, money broking, financial advisory, payment systems and instruments and foreign exchange activities may be regulated by BNM under the Malaysian Financial Services Act 2013 (FSA), and its related regulations, directions, notices, guidelines and industry codes. Fintech/insurtech activities involving the money changing and remittance services may be regulated by BNM under the Malaysian Money Services Business Act 2011.

BNM had, in 2014, issued an announcement stating that Bitcoin (and likely, by extension, other virtual currencies) is not legal tender and that BNM does not regulate the operation/use of Bitcoin.

Any activities that relate to the dealing with derivatives, securities, fund management, advising on corporate finance, as well as providing investment advice and financial planning services may be regulated under the Malaysian Capital Market and Services Act 2007 (CMSA). The SC has issued guidelines to regulate the crowdfunding sector (both equity and peer-to-peer), and more recently, revised various guidelines to regulate digital investment management (robo-advice). Note that financial exchange derivatives fall within the purview of BNM.

To the extent that the activities relate to cryptography and data encryption, and the export of cryptographic/data encryption technology, the activities may be subject to regulation under the Malaysian Strategic Trade Act 2010.
What are the types of fintech/insurtech activities that are regulated?

**MYANMAR**

In relation to fintech, a license from the Central Bank of Myanmar (CBM) is required for an institution to provide e-money (monetary value stored on a card), credit tokens (credit cards) and mobile financial services.

Except to the extent that insurtech activities fall within those services, insurtech is otherwise not addressed under current Myanmar law. However, as the insurance market is still heavily regulated, any activities that relate to insurance can only be undertaken with the approval of the Ministry of Planning and Finance, and only within the permitted scope of the allowed insurance products.

**PHILIPPINES**

The use by BSP-regulated entities of information technology in the provision of their services is subject to the BSP Guidelines on Information Technology Risk Management for All Banks and Other BSP-Supervised Institutions. Other than this and the regulations on e-money, remittance/money transfer services, and virtual currencies used for delivery of financial services (for example, payments and remittances), to date, the BSP has not yet issued regulations specifically on fintech activities. However, there are pending bills in the Philippine Congress that seek to regulate online and non-traditional payment systems and vest on the BSP regulatory powers over those payment systems.

Similarly, to date, the SEC has not yet issued regulations specifically on fintech activities in the capital markets sector.

With respect to the insurance sector, the buying, selling, or providing of insurance products and services online or via the internet are subject to the Guidelines on Electronic Commerce of Insurance Products issued by the Insurance Commissioner in 2014. Other than this, to date, the Insurance Commission has not yet issued regulations specifically on fintech activities of insurance companies and insurance intermediaries.

Given the absence of specific regulations on fintech activities in the banking, capital markets and insurance sectors, a person wishing to introduce a fintech product or service will need to confer with the regulator to get confirmation on whether the product or service may be introduced in the Philippines. Based on our experience, regulators are generally receptive to the introduction in the Philippines of fintech products and services that have been introduced in many other countries, subject to the regulator’s imposition of certain conditions for the protection of the public. The process of obtaining such regulatory confirmation/approval usually takes time, and the grant of confirmation/approval is subject to the regulator’s sole discretion.
What are the types of fintech/insurtech activities that are regulated?

<table>
<thead>
<tr>
<th>SINGAPORE</th>
</tr>
</thead>
</table>
| Activities involving insurers, insurance intermediaries and the insurance business may be regulated under the Insurance Act (Cap. 142), Financial Advisers Act (Cap. 110), and their attendant regulations, directions, notices, guidelines and industry codes (for example, there are codes of conduct or guidelines under the auspices of the General Insurance Association (GIA) or the Life Insurance Association (LIA)). Regulated insurance companies seeking to commence or develop fintech/insurtech activities must ensure that any new activities comply with the foregoing (as applicable) and do not breach any existing license conditions. In order to encourage more fintech/insurtech experimentation, the MAS has implemented the regulatory sandbox experiment such that companies may avail themselves of a regulatory sandbox to experiment with fintech solutions in the production environment but within a well-defined space and duration.

Payment and settlement systems (for example, digital payments) may be regulated under the Payment Systems (Oversight) Act (Cap. 222A), its attendant regulations, directions, notices and guidelines. Money-changing and remittance businesses will be subject to the requirements of the Money-changing and Remittance Businesses Act (Cap. 187), its attendant regulations, directions, notices and guidelines.

In August 2016, the MAS issued a Consultation Paper on Proposed Activity-based Payments Framework and Establishment of a National Payments Council. This consultation proposes a payment framework that will supersede the Payment Systems (Oversight) Act (Cap. 222A), and envisages regulation on an activity basis to entities within the payments ecosystem to allow MAS to better address issues such as consumer protection, access, corporate governance, and other emerging risks such as cybersecurity, interoperability, technology, and money-laundering and terrorism financing.

Virtual currencies (for example, Bitcoin) are not regulated; however, the MAS has announced that virtual currency intermediaries may be regulated for anti-money laundering and countering the financing of terrorism purposes.

Any activities involving all offers of investments of securities in Singapore (for example, equity crowdfunding platforms), the dealing of securities, fund management, securities financing, custodial services for securities, leveraged foreign exchange trading, trading in futures contracts, among others, will potentially be regulated under the Securities and Futures Act (Cap. 289). Fintech activities involving moneylending may also be regulated under the Moneylenders Act (Cap. 188).

Separately, in relation to cryptography and data encryption, while Singapore does not have control on the import of cryptographic/data-encryption products or their use, the export of cryptographic/data-encryption products and technology listed in the Strategic Goods Control List of the Strategic Goods (Control) Order 2015, is controlled under the Strategic Goods (Control) Act (Cap. 300).
### Taiwan

Activities involving insurance companies, insurance agents or brokers and insurance businesses may be regulated under the Insurance Act, the Regulations Governing Insurance Agents, the Regulations Governing Insurance Brokers, relevant rulings and rules and guidelines promulgated by the Non-Life Insurance Association, the Life Insurance Association, the Insurance Agents Association and the Insurance Brokers Association.

Payment and settlement systems may be regulated under the Banking Act, the Act Governing Issuance of Electronic Stored Value Cards, the Act Governing Electronic Payment Institutions and relevant regulations and rulings.

Fund remittance businesses will be subject to the Banking Act, the Act Governing Electronic Payment Institutions and the Foreign Exchange Regulation Act.

Virtual currencies (for example, Bitcoin) are not recognized by Taiwan governments. On 30 December 2013, the Central Bank of Taiwan issued a press release warning against the risks of using Bitcoin.

Activities involving investments of securities, the dealing of securities, fund management, trading in futures contracts, among others, will be regulated under the Securities Exchange Act, the Futures Trading Act and the Securities Investment Trust and Consulting Act.

On 12 January 2017, the FSC published the Draft Bill of the Act of Financial Technology Innovation Experiment (the Draft Fintech Act), which sets out the guidelines to launch and implement a regulatory sandbox in Taiwan. The Draft Fintech Act was approved by the Executive Yuan on May 4, 2017, and it will be submitted to the Legislative Yuan for its first reading in Autumn 2017. The purpose of the Draft Fintech Act is to encourage financial institutions and fintech service providers to improve the efficiency and quality of financial services by developing innovative technologies. The Draft Fintech Act offers a financial institution or a fintech service provider, which is approved by the FSC under the Draft Fintech Act (the Applicant), regulatory flexibilities and a safe environment to conduct innovative fintech experiment (the Innovative Experiment) within a maximum period of 12 months. During such period, the applicant will be exempted from certain administrative and criminal liabilities under current financial regulations.

### Thailand

Activities involving insurers, insurance intermediaries and the insurance business may be regulated under the Life Insurance Act B.E. 2535 (1992), as amended, and the Non-Life Insurance Act B.E. 2535 (1992), as amended, and subordinate legislation issued by the OIC.

Regulated insurance companies seeking to commence or develop fintech/insurtech activities must ensure that any new activities comply with the foregoing (as applicable) and do not breach any existing license conditions. In order to keep pace with the rapid changes, the OIC has approved the utilization of a regulatory sandbox in Thailand to enable insurers, agents, fintech/insurtech players to beta test insurtech innovations.

For financing-related activities, financial services in Thailand are a very heavily regulated sector. When offering fintech/insurtech products and services to the Thai market, the key questions that need to be answered are whether the business operator will be able to operate legally in Thailand and whether a license, registration or approval is required, such as a banking license, e-payment license, securities license, personal loan license, credit card business license, FX license, money transfer license, crowdfunding portal approval, etc.

Securities-related business is also subject to licensing requirements by the SEC.
What are the types of fintech/insurtech activities that are regulated?

**VIETNAM**

There is no single comprehensive or specific law on fintech/insurtech, but depending on the areas involved, such activities may be governed by relevant existing laws.

In principle, fintech/insurtech business must first observe the general regulations, such as the Civil Code, the Commercial Law, the Law on Enterprises, the Investment Law and other specialized regulations.

Activities involving insurance business of insurers and insurance brokers in Vietnam may be governed by or regulated under the Law on Insurance Business and its implementing regulations.

Activities involving credit institutions in relation to financial and banking services, including payment, money exchange, moneylending and remittance businesses, may be subject to, among others, the Law on Credit Institutions and the Ordinance on Foreign Exchange Control and their specific implementing regulations.

Activities involving securities companies and fund management companies may be governed by or regulated under the Securities Law and its specific implementing regulations.
### AUSTRALIA

The Australian government is supportive of insurtech. Through ASIC’s regulatory sandbox, non-insurance tech entrants and insurtech start-ups are exempt from licensing requirements in relation to products that are subject to appropriate monetary exposure limits (AUD 50,000 for retail clients and AUD 5 million for wholesale clients), such as:

- home contents insurance products (for example, household goods and jewelry)
- personal and domestic insurance products (for example, mobile phone insurance)

ASIC may further exempt other regulatory requirements with the use of its waiver (relief) powers on a case-by-case basis when appropriate.

That said, the insurance industry largely feels that insurtech has been somewhat left behind in terms of the fintech agenda in Australia, and sees scope for the Australian government to further reduce regulatory barriers. In particular, the industry has asked the Australian government to support increased flexibility, which in turn supports emerging micro-insurance and quasi-insurance models, which are not easily operated under current models.

### CHINA

While there has been strong government and regulatory support for fintech/insurtech, Chinese regulators have become more and more cautious about the potential risks posed by these businesses and may impose stricter and broader regulation on various fintech/insurtech businesses.

The significance of fintech/insurtech has been recognized and endorsed by the Chinese government. For example, the Fintech Guidelines provided strong policy direction for supporting and promoting the development and growth of fintech in China. Specifically, the Fintech Guidelines set out the following goals of the Chinese government:

- promoting innovation of fintech platforms, products and services
- encouraging cooperation between financial institutions and internet companies
- improving access to capital for fintech firms through the promotion of venture capital, SME finance and public listings
- streamlining administrative approvals for fintech firms
- providing tax benefits for fintech/insurtech start-ups and fintech innovations
- encouraging the development of credit information infrastructure and supporting service systems for fintech/insurtech

However, with more and more reported cases of fraudulent or problematic P2P lending platforms in 2015, it has been reported that Chinese regulators are in the process of drafting new rules to tighten up the control over certain fintech/insurtech businesses such as internet lending, internet payment and internet insurance businesses. Many companies conducting internet lending, internet payment or internet insurance businesses have been closed down or had their operating licenses revoked since 2015.
### HONG KONG

Hong Kong regulators have reacted positively and encourage fintech/insurtech innovation in the following ways:

- **Funding** – The Hong Kong government has already made available an Enterprise Support Scheme under the Innovation and Technology Fund to encourage private sector investment in research and development activities. Funding up to HKD 10 million for each approved project would be provided on a matching basis, with no requirement for recoupment of the approved grant. Together with other similar funding schemes by government, a pool of about HKD 5 billion is available for ventures and research projects in various technology areas, including fintech/insurtech.

- **Support** – The IA, the HKMA and the SFC have set up dedicated fintech/insurtech platforms to help enhance communication between regulators and the fintech/insurtech community. Such platforms handle inquiries from the industry and provide information on related regulatory requirements to companies engaging in financial innovation. The platforms will also keep track of the latest development in the market through their exchange with the industry.

- **Policy views** – The Hong Kong government has indicated that, in developing fintech/insurtech, it will uphold the "technology neutrality" principle and at the same time attach importance to investor protection. The government will help ensure that there is an appropriate balance between market innovation and investors’ understanding and tolerance of risks. The government also indicated that the existing regulations are adequate to handle the challenges from the growing fintech/insurtech sector in Hong Kong.

- **Developing expertise** – The HKFI has recently set up a task force on Financial Technology Hub. It is exploring how to work with the government to promote innovation in the insurance industry, including attracting capital and talent.

### INDONESIA

Although there are no specific fintech/insurtech regulations, the government is aware of technological developments and is now encouraging fintech/insurtech activities and has acknowledged that a regulatory framework needs to be put in place.
### 3. What is the attitude and what are the policy views of the regulator in relation to insurtech (if any)? Is innovation encouraged?

<table>
<thead>
<tr>
<th>Country</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>JAPAN</strong></td>
<td>The FSA is supportive of the introduction of fintech/insurtech and intends to strongly support fintech/insurtech start-ups. The Financial Administration Policy for 2015-2016 issued by the FSA in September 2015 expressly states that the FSA will anticipate the trend of fintech/insurtech and will prepare the environment so that technological innovation can contribute to economic and financial development in Japan. The Financial Administration Policy for 2016-2017 issued by the FSA in October 2016 also states that the movement of integration of finance and IT represented by fintech has been progressing on a global scale and revolutionizing both financial services and market and that it is important to provide better services through innovation of financial services in Japan (collectively, Financial Administration Policy). Based on the Financial Administration Policy, the FSA established the Fintech Support Desk in December 2015 to serve as point of contact for consultation and information exchange on financial regulations regarding fintech. The FSA also established the Expert Panel on FinTech Venture in April 2016 to discuss desirable environment for development of fintech. The METI is also supportive of the introduction and promotion of fintech/insurtech-related businesses to the Japanese market. The METI has held a series of meetings of Study Group on the Integration of Industry, Finance and IT (Study Group) since October 2015. The METI started to seek public comments on 11 agenda items identified relating to fintech on 21 April 2016 and the public comments period ended on 23 May 2016. Since 1 July 2016, the METI has started to hold a series of meetings of Review Committee for Issues and Future Direction of FinTech (FinTech Review Committee). The METI put together the discussions held in the FinTech Review Committee and issued the final report titled &quot;FinTech Vision&quot; in May 2017.</td>
</tr>
<tr>
<td><strong>MALAYSIA</strong></td>
<td>The regulators have been positive and encourage fintech/insurtech innovation. The SC has adopted a collaborative approach. In September 2015, the SC launched the aFINity@SC initiative (that is, the Alliance of FinTech Community) to create a network for fintech stakeholders to engage with the SC. More importantly, the SC intends to introduce policy and provide regulatory clarity for fintech/insurtech businesses through aFINity@SC. The SC also intends to work together with relevant fintech-related stakeholders, including innovators, entrepreneurs, established businesses, investors and other authorities, as part of a concerted effort to accelerate growth and innovation in the financial industry. The SC will function as the network organizer in pursuing key deliverables, which include (i) creating awareness and catalyzing development in fintech; (ii) forming hubs to organize and nurture a wider fintech/insurtech ecosystem; and (iii) providing policy and regulatory clarity that is conducive for innovation. In June 2016, BNM established the Financial Technology Enabler Group (FTEG), which is responsible for the regulatory framework to facilitate fintech in the Malaysian financial services industry. FTEG demonstrates BNM's commitment toward supporting fintech innovations for a progressive financial services sector. BNM has also shown awareness of fintech initiatives in the industry. For example, BNM launched the Financial Technology Regulatory Sandbox Framework in October 2016 to allow regulatory flexibilities to be granted to financial institutions and fintech companies to experiment with fintech solutions in a live controlled environment with appropriate safeguards for a limited period of not more than 12 months. The initiatives by the FTEG will complement other initiatives by BNM, for example, regulating the establishment and operations of the product aggregators in the insurance sector and launching the Market Development Fund framework to impose annual targets of point-of-sale terminals in Malaysia to be achieved by participating card organizations in collaboration with payment system operators.</td>
</tr>
</tbody>
</table>
### MYANMAR

Currently innovation in the insurance market is not possible. There are a small number of licensed insurance providers who are permitted to offer a set range of insurance products (that is, there is no product differentiation).

We understand that when the new insurance market regulations are released, they will promote significantly increased flexibility and competition in the insurance market, including significant opportunity for innovation and the ability to invest in and promote insurtech. At this point in time, there is no clear time frame for the relaxation of the Myanmar insurance market; however, we consider that it is likely to be sometime in late 2017 or early 2018.

### PHILIPPINES

Based on our experience, regulators are generally receptive to the introduction in the Philippines of fintech products and services that have been introduced in many other countries, subject to the regulator’s imposition of certain conditions for the protection of the public.

Regulators view fintech as a way of pursuing financial inclusion through digital technology. Having said that, the process of getting such regulatory confirmation/approval of a fintech product or service that is not specifically governed by existing laws and regulation usually takes time, and the grant of confirmation/approval is subject to the regulator’s sole discretion.

In the case of the BSP, for example, it is known for encouraging innovations in financial services. As an example, with the advent of e-money in the Philippines, the BSP has established a new supervisory unit bringing together the skills of regulators from its information technology area as well as the banking supervisory area. Through this newly established supervisory unit, the BSP strengthened its regulatory capacity to oversee e-money issuers. The BSP is closely monitoring the progress of fintech/insurtech in the Philippines and its impact on the local banking industry.

The IPOPHL fully supports technological innovation, including financial technologies. To this end, the IPOPHL has established a nationwide network of Innovation and Technology Support Offices, which assists local innovators in claiming and protecting their intellectual property rights.
### What is the attitude and what are the policy views of the regulator in relation to insurtech (if any)? Is innovation encouraged?

<table>
<thead>
<tr>
<th>Country</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SINGAPORE</td>
<td>There is strong government and regulatory support. The development of the fintech/insurtech space is in line with Singapore’s ambition to be a Smart Nation. The MAS seeks to create a Smart Financial Centre where technology is used pervasively in the financial industry to increase efficiency, create opportunities, allow for better management of risks and improve lives. Fintech/insurtech, which involves using technology to devise new financial services and products, is a key ingredient in building a Smart Financial Centre. The regulators have been positive and encourage fintech/insurtech innovation in the following ways:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Funding</strong> – There are currently various funding schemes for fintech/insurtech-related innovations. In particular, the MAS has committed SGD 225 million to the Financial Sector Technology &amp; Innovation scheme (FSTI), which is aimed at growing the fintech/insurtech ecosystem in Singapore over the next five years by funding the establishment of innovation labs, institutional-level projects and industry-wide initiatives. Some FSTI-supported projects include a decentralized record-keeping system that prevents duplicate invoicing in trade finance, a cyber-risk test bed and a natural catastrophe data analytics exchange. The MAS is providing up to SGD 1.15 million worth of prizes (to a maximum of 10 winners) through the FTSI scheme to recognize innovative fintech solutions that have been implemented.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Support</strong> – The MAS, together with the National Research Foundation, has set up a FinTech Office to serve as a one-stop virtual entity for all fintech/insurtech matters and to promote Singapore as a fintech/insurtech hub. The new FinTech Office will assist with reviewing, aligning and enhancing these funding schemes across government agencies, identify gaps and propose strategies, policies, and schemes in industry infrastructure, talent development and manpower requirements, and business competitiveness, and manage the branding and marketing of Singapore as a fintech/insurtech hub through fintech/insurtech events and initiatives. The inaugural Singapore Fintech Festival that was held in Singapore from 14 to 18 November 2016 — the first of its kind in Asia — is a good example of Singapore’s commitment to promote itself as a fintech/insurtech hub. The festival showcased, among other things, a selection of up to 20 teams that were invited to ideate and co-create solutions to specific problems/challenges faced in the financial industry. The MAS has also announced the second edition of the Singapore Fintech Festival, which will be held from 13 to 17 November 2017.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Policy views</strong> – Recognizing that innovation may be constrained by existing regulations, the MAS indicated that it does not expect financial institutions to seek MAS approval for all new digital products and services. Instead, they may proceed to launch such products without MAS approval provided that they are satisfied with their due diligence that no license or approval is required in relation to such products. In terms of the regulatory approach, the MAS will apply a materiality and proportionality test and ensure that regulation must not front-run innovation. To further this policy, the MAS, in November 2016, issued the FinTech Regulatory Sandbox Guidelines, which seek to encourage more fintech experimentation so that promising innovations can be tested in the market and have a chance for wider adoption in Singapore and abroad. Approval to enter the regulatory sandbox should be sought when experimenting with innovative financial services in the production environment, and the MAS may determine the specific legal and regulatory requirements, which it is prepared to relax for each case.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Developing expertise</strong> – The MAS has also set up the Financial Technology and Innovation Group within the MAS comprising three divisions (two of which — the Payments &amp; Technology Solutions Office and the Technology Infrastructure Office — would focus on the regulatory policies, whereas the third — the Technology Innovation Lab — would focus on innovation and keep a lookout for opportunities to cooperate with the industry to test bed innovative solutions). This would allow the MAS to ensure that rather than having its regulations play catch-up with innovation, the MAS would stay very much involved and engaged in innovation in order to better supervise and regulate.</td>
</tr>
</tbody>
</table>
What is the attitude and what are the policy views of the regulator in relation to insurtech (if any)? Is innovation encouraged?

<table>
<thead>
<tr>
<th>TAIWAN</th>
<th>To engage fintech/insurtech innovation by the financial institutions, the FSC adopted the following policies:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Allowing financial industry to invest in fintech/insurtech enterprises – The FSC has announced the relevant regulation, allowing banks and financial holding companies to invest in financial technology companies, including companies specializing in big data, cloud computing, biometrics, robo-adviser, among others, and to hold up to 100% of the equity shares of the companies. The FSC has allowed insurance companies, securities firms, securities investment trust enterprises (SITEs), securities investment consulting enterprises (SICEs) and domestic futures commission merchants, within certain limits, to invest in business-related or auxiliary to fintech/insurtech-related business.</td>
</tr>
<tr>
<td></td>
<td>• Promoting fintech/insurtech development</td>
</tr>
<tr>
<td></td>
<td>(a) Publishing of the Financial Technology Development Policy White Paper – To master the development of network and international trend of financial technology application, the FSC published the Financial Technology Development Policy White Paper in January 2015 as Taiwan’s fintech blueprint revealing the international trend, the current domestic situation, policy goals and strategies.</td>
</tr>
<tr>
<td></td>
<td>(b) Promoting the e-payment ratio multiplication five-year plan – In order to enhance the efficiency of payment, save the cost of cash payment processing, stimulate economic growth through consumer spending, reduce the scale of the underground economy, increase financial transparency, reduce the circulation of false money, and lower the crime rate, the FSC is promoting the domestic e-payment. Through both government and private sector, and the combination of finance and technology, the ratio of e-payment will be doubled in the next five years, compared to recent 26% ratio.</td>
</tr>
<tr>
<td></td>
<td>(c) Encouraging insurance companies to design innovation products by using big data, such as usage-based insurance</td>
</tr>
</tbody>
</table>
What is the attitude and what are the policy views of the regulator in relation to insurtech (if any)? Is innovation encouraged?

| Thailand |
The regulators have been positive and encourage fintech/insurtech innovation in the following ways:

- **Crowdfunding** – Further to the notification in relation to equity-based crowdfunding issued by the SEC, effective since 16 May 2015, which allows a qualified company to raise funds from the public by offering shares through an electronic platform provided by a funding portal approved by the SEC, the SEC is currently holding a public hearing regarding the revision to be made to the notification to further facilitate the fintech innovation. The key revised principles include (i) allowing the funding portal to use technologies, for example, blockchain, smart contract in managing shares subscription’s money, instead of requiring the funding portal to have an escrow agent, an intermediary, or a reliable person to keep the member’s assets; (ii) allowing the funding portal to act as a secondary market by providing an e-trading platform to enable shares offered through funding portals to be traded, in order to provide more exit options for investors; and (iii) removing the current restriction that requires the company raising funds through a funding portal to use such same funding portal in the next fundraising rounds. The public hearing is open for comments until 23 August 2017.

- **Payment system law** – A draft new payment system law, intended to reform and unify the laws in relation to payment systems in Thailand, was approved in the third reading by the National Legislative Assembly on 10 August 2017 and is pending only the last process of being published in the Royal Gazette in order to become a law. According to this final draft, this draft involves the key payment systems important to the security of the financial system (and the payment finality concept) as well as the payment system under supervision (where new requirements include, for example, protection of float money in case of the business operator’s insolvency).

- **National e-Payment Master Plan** – The Cabinet approved the Master Plan in principle on 22 December 2015, showing the recognition and intention to drive the transformation of Thailand’s payment system to full electronic payment infrastructure both in the government and private sectors. It is hoped that the Master Plan will bring about payment infrastructure development (for example, any ID payment system), e-tax system, e-payment system for social welfare, financial inclusion, and a cashless society, the environment in which fintech businesses will likely thrive.

- **Regulatory Sandbox** – On 9 May 2017, the OIC launched a new notification on insurance regulatory sandbox, which would support the development of new innovations and allow applicants to experiment on new innovations within a more flexible regulatory requirement as deemed appropriate by the OIC.

- **FinTech Challenge** – In July 2017, the SEC, the OIC, the BOT and other six authorities launched a contest opening up opportunities for new start-up companies to present fintech/insurtech innovations. Categories of this contest include Customer-Centric, RegTech, and Infrastructure. This initiative is introduced with an aim to support and encourage new fintech/insurtech innovations.

- **Others** – It is also expected that there will be continued developments in other laws and regulations relevant to the operation of fintech/insurtech businesses such as anti-money laundering law, exchange control law and data protection law.
VIETNAM

The Vietnamese government is aware of technological developments and it encourages fintech/insurtech activities. However, some laws and regulations would need to be adjusted or developed for fintech/insurtech activities. The authorities, such as the SBV and the MOF, may take a conservative view in granting relevant approval and license.

- Developing corresponding legal framework for fintech activities in Vietnam – To keep up with the development of fintech in Vietnam, regulators have gradually improved and updated its legal framework, with consideration of developments of fintech/insurtech activities, including regulations on e-commerce activities and intermediary payment services. In relation to the insurance industry, under the recently issued new decree, the sale of insurance products “via electronic transactions” is added into the possible channels that local insurers can use for sale of insurance products. This is expected to provide a legal basis to recognize online distribution channel and promote fintech activities in the insurance market.

- Supporting and funding – Vietnamese authorities are aware of the rapid development of fintech/insurtech activities in Vietnam. For the first time in Vietnam, the MOST and the government of Vietnam took the initiative of stimulating the growth of technology start-ups in Vietnam by launching the project “Silicon Valley Ecosystem in Vietnam.” The project seeks to create an ecosystem of innovations and technology commercialization in Vietnam.

Nonetheless, insurance, banking and other financial services are sensitive areas that need to be regulated. Although some authorities remain rather supportive, the SBV and the MOF usually take more conservative views toward technology development in the insurance, financial and banking sectors. For instance, the SBV specifically disallows all use of virtual currency as a payment method, including Bitcoin, in Vietnam.

Generally, the government encourages fintech/insurtech innovation in Vietnam. Yet, given that insurance, banking and finance are considered sensitive areas in Vietnam, the authorities such as the SBV and the MOF may take a conservative view in granting relevant approval and licenses.
The licenses required will depend on the specific activities contemplated. The key licensing and/or regulatory requirements include:

- **Financial services or credit licenses** – Businesses conducting a financial services business or providing credit require the relevant financial services or credit licensing conditions from ASIC.
- **ASIC regulatory sandbox exemption** – Businesses that qualify under ASIC’s regulatory sandbox may apply to ASIC to have their licensing requirements waived. As discussed (at question 2), eligible start-ups that qualify to operate under ASIC’s regulatory sandbox may operate for 12 months without needing to apply for a financial services or credit license, provided that products and services are offered to wholesale clients and a limited number of retail clients (up to 100 retail clients only), with appropriate monetary exposure limits in place. ASIC may further use its waiver (relief) powers on a case-by-case basis.
- **Authorized deposit-taking institution (ADI)** – Institution seeking to be regulated as an ADI will require the relevant licenses with APRA.
- **Equity crowdfunding** – Companies looking to facilitate capital raising under the Australian government’s latest crowdsourced equity funding framework starting in September 2017 will require a financial services license. Among other things, this allows eligible companies to raise up to AUD 5 million per year if they have less than AUD 25 million in gross asset value.
- **Venture capital** – Fintech/insurtech investors may apply to Innovation Australia to be structured as a venture capital limited partnership (VCLP), or early-stage venture capital limited partnerships (ESVCLP) under the Venture Capital Act 2002 (Cth) and receive more favorable tax treatment for investment.

**CHINA**

Depending on the specific activities involved, the following licensing and/or regulatory requirements may be triggered for:

- conducting an Internet banking business – a financial license is required
- conducting Internet payment services – a payment business license is required
- Internet lending business: (i) Internet small-amount lending business is subject to the requirements of provincial-level finance office; (ii) for P2P online lending, the P2P online lending platform is required to serve as intermediary only and must choose a qualified banking financial institution as the capital depository institution for both the lenders and the borrowers.
- conducting equity crowdfunding business, registration and membership with the Securities Association of China is required
- conducting Internet fund sales, a publicly raised fund sales payment and settlement institution license is required.
- conducting Internet insurance sales, an insurance license is required. However, for insurance sales through third-party platform, no license (other than the relevant telecommunication license or recordal) is required for the third-party platform.
- conducting Internet trust business or Internet consumer finance, a financial license is required.

In addition, the relevant telecommunication license or recordal is also required for operating the online platform for providing the relevant fintech/insurtech.
What are the licenses required and what are the criteria and process involved?

The licenses required will depend on the specific activities contemplated. We recommend seeking advice of local counsel. In brief overview:

- Designated Retail Payment Systems. The HKMA does not operate a licensing system for RPS. However, for a RPS which is designated by the HKMA, the operator needs to ensure that (a) the operations of the system are conducted in a safe and efficient manner; (b) there are operating rules that comply with the prescribed requirements; (c) there are adequate arrangements to monitor and enforce compliance with the operating rules of the system; and (d) financial resources appropriate for the proper performance of the system's particular functions are available to the system.

- Stored Value Facilities. The HKMA operates a licensing system for multi-purpose stored value facilities (SVF) (that is, an SVF which serves as a means of payment for goods and services provided by participating merchants, which is akin to an electronic surrogate for coins and banknotes). Such licensing regime covers both "device-based" SVF (for example, the value is stored in an electronic chip on a card) and "non-device based" SVF (for example, a network based account where the value is stored). There are certain licensing exemptions (for example, a SVF that is used for certain cash reward or bonus point schemes). Also, a license is not required for the issuance of a single purpose SVF (for example, a SVF which can only be used as a means of prepayment for goods and services provided by a merchant, and such merchant is also the issuer of the SVF).

- Remittance business. A money service operator license may be required for remittance business.

- Equity Crowdfunding. Depending on the nature of the crowdfunding activity, crowdfunding platform operators may be required to be licensed under the Securities and Futures Ordinance (Cap. 571) for the following types of regulated activities: Type 1 (dealing in securities); Type 4 (advising on securities); Type 6 (advising on corporate finance); Type 7 (providing automated trading services); Type 9 (asset management). In addition, crowdfunding activity may trigger the restrictions under the offer of investment regime under the Securities and Futures Ordinance (Cap. 571) and the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32).

- Moneylending. A moneylender’s license may be required if the contemplated activity is not excluded or exempt under the Money Lenders Ordinance (Cap. 163).

- Telecommunications License. Under the Telecommunications Ordinance (Cap. 106), there are prohibitions against establishing or maintaining any means of telecommunications or offering in the course of business a telecommunications service. Licenses will need to be obtained from the Communications Authority for such activities, unless the relevant exemptions under the ordinance apply.

- Intellectual property registrations. For completeness, if the fintech/insurtech innovation involves a patentable invention or if there are plans to register a trademark, further information can be found at the following links:
  (d) For patents: (http://www.ipd.gov.hk/eng/applicants/patents.htm)
  (e) For trademarks: (http://www.ipd.gov.hk/eng/applicants/trademarks.htm)

Please note that the foregoing links may be updated from time to time and you are advised to check with local counsel for updates before relying on the above information.
The licenses required will depend on the specific activities contemplated:

- **Insurance.** In the absence of a specific regulation on insurtech, no specific license is required if an insurance company sells an e-policy.
- **Insurance broker.** An insurance broker business must obtain a business license from the OJK (whether services are offered through digital channels or not).
- **E-money.** Licenses for e-money activities must be obtained from Bank Indonesia.

Licensing from Bank Indonesia is bureaucratic and the existing regulations were introduced some time ago and are convoluted. One of the requirements to become an e-money operator is that the applicant must be a limited liability company, whether it is a foreign investment company (majority or wholly owned) or a pure local company. In the licensing process, Bank Indonesia will review the submitted documents, verify the validity of information set out in them and conduct a site visit to see an applicant’s readiness to become an e-money operator. During the review and verification process, Bank Indonesia may require an applicant to have a meeting with Bank Indonesia to elaborate on the e-money product that will be offered in Indonesia and other aspects relating to provision of the product. If Bank Indonesia is satisfied with what an applicant presents, Bank Indonesia will issue an e-money business license. Under the e-money regulations, there is no specific timeline for Bank Indonesia to issue an e-money business license.

Bank Indonesia has the authority to open, close and limit e-money licensing at its discretion, for example, for the purposes of maintaining national efficiency, provisions of public services and fair business competition.

- **Remittance business.** Licenses for remittance activities must be obtained from Bank Indonesia.
- **Crowdfunding:** Public crowdfunding activities require an effective statement from the OJK.
- **Intellectual property registrations.** For completeness, if the fintech/insurtech innovation involves a patentable invention or if there are plans to register a trademark, investors need to register matters.
The licenses required will depend on the specific activities contemplated. We recommend seeking the advice of local counsel as it is even difficult to identify under which regulations a particular activity should be regulated. In brief overview:

- **Insurance business.** A license may be required to perform life or non-life insurance business. The criteria to obtain the license are specified under the relevant provisions in the Insurance Business Act and the Ordinance for Enforcement of the Insurance Business Act. The standard processing period designated under the relevant regulations is 120 days. A license may be also required to create new insurance products. The criteria to obtain the license are specified under the relevant provisions in the Insurance Business Act. The standard processing period designated under the relevant regulations is 90 days. However, the Comprehensive Guidelines for Supervision of Insurance Companies (Insurance Supervision Guidelines) express that the FSA shall endeavor to reduce the review period in light of assistance in prompt product development. In particular, it is expressed that stylized and simple products and the products that are substantially the same as the other companies’ existing products shall be, in principle, reviewed within 45 days.

- **Insurance broker business.** A registration may be required to run a insurance broker business. The criteria to be registered are specified under the relevant provisions in the Insurance Business Act. The standard processing period designated under the relevant regulations is 30 days.

- **Accepting deposits.** In order to accept deposits from customers, a license may be required. The criteria to be registered are specified under the relevant provisions in the Banking Act and other Ordinance for Enforcement of the Banking Act. The standard processing period designated under the relevant regulations is one month.

- **Money lending and credit provision for settlement.** In order to perform moneylending and credit provision for settlement (including credit card), a license or registration may be required depending on the type of activities. For banking business license, please see item 3 above. For moneylending business, the criteria to be registered are specified under the relevant provisions in the Money Lending Business Act. The standard processing period designated under the relevant regulations is two months. For credit provision for settlement, the criteria to be registered are specified under the relevant provisions in the Installment Payment Act. The standard processing period designated under the relevant regulations is 60 days.

- **Prepaid card or other prepaid type of service.** Issuers of prepaid payment instruments for third-party business need to be registered. The criteria to be registered are specified under the relevant provisions in the Payment Services Act. The standard processing period designated under the relevant regulations is two months.

- **Funds transfer service.** In order to run a fund transfer service, a license or registration may be required depending on the monetary amount to be transferred. For banking business license, please see item 3 above. For fund transfer service providers under the Payment Service Act, the criteria to be registered are specified under the relevant provisions in the Payment Service Act. The standard processing period designated under the relevant regulations is two months.

- **Investment advisory and investment management business.** In order to perform investment advisory or investment management business, a registration may be required. The criteria to be registered are specified under the relevant provisions in the FIEA. The standard processing period designated under the relevant regulations is two months.
Crowdfunding. A registration as type II financial instruments business operator may be required for crowdfunding made through collective investment scheme. The criteria to be registered are specified under the relevant provisions in the FIEA. The standard processing period designated under the relevant regulations is two months.

Virtual currency exchange. In order to perform virtual currency exchange business, a registration may be required. The criteria to be registered are specified under the relevant provisions in the Payment Services Act. The standard processing period designated under the relevant regulations is two months.

The licenses required will depend on specific activities that are contemplated. The relevant licenses that may be required include, among others:

- Banking or insurance licenses and approvals for other approved businesses. No person may carry on banking or insurance businesses or any other approved businesses such as the operation of a payment system, issuance of a designated payment instrument, money-brokering businesses or financial advisory businesses without a license or an approval from BNM. However financial technology companies (approved by BNM under the Financial Technology Regulatory Sandbox Framework issued by BNM) are exempt from obtaining licenses required under the FSA and IFSA to carry out, among others, banking and insurance businesses.

- Capital market services license. No person may carry on a business in any of the regulated activities (which include dealing with derivatives, dealing with securities, fund management, advising on corporate finance, providing investment advice and financial planning services) unless licensed by the SC. Individuals undertaking such activities must also obtain a capital market services representative license from the SC. It should be noted that the SC also introduced a new category of capital market services license for fund management companies which undertake discretionary portfolio management by incorporating innovative technologies (robo-advice).

- Crowdfunding license. Any person carrying on a crowdfunding business (including peer-to-peer crowdfunding/lending activities) must be licensed by the SC.

- Moneylending license. Any person undertaking moneylending services must be licensed by the Ministry of Housing and Local Government, unless exempted.

- Money services license. Any person engaged in the money-changing or remittance businesses must be licensed by BNM.

- MCMC license. Network services, network facilities, application services and content application services providers must be licensed by the MCMC.

- Intellectual property registrations. Trademark and/or patent registrations can be filed for fintech/insurtech innovations, which involve a patentable innovation or which can be registered as a trademark with MyIPO. Depending on whether there are any objections raised to such registrations, it may take between 1 and 1.5 years to register a trademark and 5 and 6 years to register a patent in Malaysia.

Save for trademark registrations, which may take between 1 and 1.5 years, and patent registrations, which may take between 5 and 6 years, it generally takes 3 to 6 months to obtain licenses and approval from the various regulators above, subject to the submission of a complete set of documents and information for the application.
### MYANMAR

In order to provide any form of insurance business within Myanmar, the insurer will be required to obtain a license from the Insurance Business Supervisory Board established under the MOPF.

Licensing is not standard form and the application must be made directly to the Insurance Business Supervisory Board, which may require significant information from the applicant regarding its experience, its financial capacity and its intended business plans.

Further, any license obtained from the Insurance Business Supervisory Board is required to specifically list out the policies that the entity is licensed to provide. Approval will also need to be obtained for:

- premiums
- policy application and claim forms
- locations of proposed branch offices within Myanmar
- any promotional or marketing materials that will be used for insurance products
- the capital investments that the insurer intends to make within Myanmar

Beyond these requirements, the Insurance Business Supervisory Board may include any conditions in the business license that it considers necessary.

There is no set time frame for obtaining an insurance license, however, from experience it is possible for the process to take up to six months depending on the nature of the services requested and the capacity of the Insurance Business Supervisory Board.
Entities engaged in fintech products/services relating to e-money and remittance services (including virtual currency exchange systems), are generally required to obtain a license or authority from the BSP.

For instance, recent BSP regulations require remittance, money changing, and/or foreign exchange dealing entities to register or reregister with the BSP, the SEC, and the Anti-Money Laundering Council Secretariat. Moreover, remittance platform providers must now conduct business in the Philippines through a locally incorporated subsidiary. These entities will also be required to obtain the BSP’s prior approval for any change in the control of the entity.

For the following activities, a financial services license must be obtained from the BSP:

- Remittance/money transfer services
- Virtual currency exchanges, if used for delivery of financial services (such as payments and remittances)
- Issuance and operations of electronic money. With respect to the use of technology, the following licenses may be required
- Value-Added Services (VAS) Provider License. Under the Telecoms Law, a VAS provider is an entity which, relying on the transmission, switching, and local distribution facilities of a local exchange or inter-exchange operator or overseas carrier, offers enhanced services beyond those ordinarily provided for by such carriers. The NTC considers as VAS the delivery of applications services, including mobile banking, electronic payments, and point-of-sale services. To register with the NTC as a VAS provider, an entity must be at least 60% Filipino-owned.
- Intellectual Property Rights Registrations. Patents, industrial designs, utility models, trademarks and service marks may be registered with the IPO. Computer programs are also entitled to copyright protection. Copyrighted works may be registered with the IPO or the National Library.

It usually takes about a month to obtain a financial service license from the BSP. With respect to insurtech, the Insurance Commission has not yet issued regulations specifically on insurtech activities.

Further, the Philippine Data Privacy Act (DPA) mandates the registration of processing systems of personal information controllers and processors which are involved in the processing of sensitive personal information of at least 1,000 individuals, whether it be of employees, clients, customers, or contractors. The current deadline for this registration requirement is on 9 September 2017.

For patents, information is available at [http://info.ipophil.gov.ph/dev/services/patents/patent-application-flow-chart](http://info.ipophil.gov.ph/dev/services/patents/patent-application-flow-chart)
For copyright, information is available at [http://info.ipophil.gov.ph/dev/services/copyright/guidelines-on-copyright-registration-and-deposit](http://info.ipophil.gov.ph/dev/services/copyright/guidelines-on-copyright-registration-and-deposit)
For trademarks, information is available at [http://info.ipophil.gov.ph/dev/services/trademark/application-process-flow-chart](http://info.ipophil.gov.ph/dev/services/trademark/application-process-flow-chart)
The licenses required will depend on the specific activities contemplated. We recommend seeking the advice of local counsel. In brief overview:

- Designated Payment Systems. No operator or settlement institution of a designated payment system may hold itself out as such unless the payment system has been designated by the MAS and annual fees are required for operators of designated systems. There are additional conduct of business and reporting obligations. There is no formal application for a license for designated payment systems. However, payment systems that may satisfy the criteria to become designated payment systems would be advised to engage the MAS on their business activities in Singapore.

- Stored Value Facilities. Holders of widely accepted stored value facility (WASVF) with an aggregate of more than SGD 30 million will need to be approved as a holder of a WASVF and an approved bank must undertake full liabilities for the stored value held. The SVF Guidelines must comply with the minimum standards. Multipurpose SVFs whose aggregate value is SGD 30 million or less and single-purpose SVFs are subject to a light touch regime where no MAS approval is required (though notification to the MAS may be required), although certain restrictions may continue to apply and they are strongly encouraged to adopt and implement the SVF Guidelines, taking into consideration the nature, size and complexity of their SVFs. Applications to be approved holders of WASVF may take between 3 and 6 months; however, we recommend engaging local counsel and the MAS as early as possible in the process.

- Remittance business. A remittance license is required for remittance business, unless exempt.

- Equity crowdfunding. A capital markets services license may be required for an equity crowdfunding platform. In June 2016, the MAS announced that it will make it easier for start-ups and small and medium enterprises to access securities-based crowdfunding. The MAS has published guidelines on advertising restrictions relating to securities-based crowd-funding and FAQs on lending-based crowdfunding.
The publication reflects the position as of November 2017. Specific advice should be obtained in this evolving and complex area.

### Moneylending
A moneylender’s license may be required if the contemplated lending activity is not excluded or exempt. Further information for applying for a moneylending license can be found at the following link: https://www.mlaw.gov.sg/content/rom/en/information-for-moneylenders.html.

### Services-Based Operator License
A company intending to lease telecommunication network elements (such as transmission capacity and switching services) from any Facilities-Based Operator (FBO) licensed by IDA to provide their own telecommunication services, or to resell the telecommunication services of FBOs to third parties will need to apply for a Services-Based Operator (SBO) License. The SBO Licenses issued by IMDA fall under two categories: the SBO (Individual) License category, where individual licensing is required for the stipulated types of operations and services; and the SBO (Class) License category where interested parties will only be required to register with IMDA before providing the stipulated types of services. In general, operators who lease international transmission capacity for the provision of their services will be licensed individually.

### Intellectual property registrations
For completeness, if the fintech/insurtech innovation involves a patentable invention or if there are plans to register a trademark, further information can be found at the following links:
(a) for patents (https://www.ipos.gov.sg/protecting-your-ideas/patent/application-process)
(b) trademarks (https://www.ipos.gov.sg/protecting-your-ideas/trade-mark/application-process)

Please note that the foregoing links may be updated from time to time and you are advised to check with local counsel for updates before relying on the above information.

### TAIWAN
The licenses required will depend on the specific activities contemplated. We recommend seeking the advice of local counsel. In brief overview:

- **Payment Services.** An entity must obtain an Electronic Payment Institution license (EPS License) if it would like to offer electronic payment services, including (i) collection and paying agent for actual transactions; (ii) stored-value services for online and offline transaction; and (iii) fund transfer among electronic payment accounts, by providing an electronic payment platform through the Internet.

- **Store-Value Facilities.** Issuer must obtain an Electronic Stored-Value Card License (E-SVC License) if it would like to issue open-loop stored-value cards that can be used for multiple purposes (to purchase products and services provided not only by the issuer but also by any third party).

- **Remittance Business.** If anyone wishes to conduct remittance service, it must have a banking license or an EPS License.

- **Equity Crowdfunding.** A securities brokerage license is required for an equity crowdfunding platform.

- **Moneylending.** If the lender is an individual (P2P lending), a license is not required. However, such P2P lending shall not include any activities in relation to issue of securities/instruments (which requires approval by the FSC) or deposit taking (which requires a banking license).
What are the licenses required and what are the criteria and process involved?

The licenses required will depend on the specific activities contemplated. We recommend seeking the advice of local counsel.

In brief overview, key licenses for financial services operation in Thailand include:

- finance company license (for accepting deposits of money, or accepting money from the public, subject to withdrawal on demand, or at the end of a specified period, other than the acceptance of deposits of money, or acceptance of money from the public in accounts to be withdrawn by checks, and of employing such money in any way, such as the granting of credits, or buying and selling of bills of exchange or any other negotiable instruments)
- personal loan license (for providing loan, accepting, buying, discount purchasing, or discount purchase subrogating a bill or any owner-transferred instrument to a natural person without stipulating the objective or having the objective to acquire goods or services, and with no objective to be used in one's own business, with no property or assets as collateral; and providing loan arising from hire purchase and leasing of goods to a natural person that the business operator does not sell in normal trade, except for cars and motorcycles)
- foreign exchange business license
- international money transfer agent license
- treasury center license
- securities license based on types of regulated businesses such as securities dealing, securities brokerage, securities advisory, securities underwriting, private fund management, mutual fund management, securities lending or short sale, and venture capital
- license for derivatives dealer, derivatives agent, derivatives advisor or derivatives fund manager
- license for electronic payment business, such as e-money provider, credit card network provider, EDC (electronic data capture) provider, transaction switching provider, clearing service provider, settlement service provider, substitute payment service provider, and provider of electronic payment through any device or network

As there are many licenses involved in the conduct of finance-related and security-related businesses in Thailand (depending on the specific fintech/insurtech activities contemplated), advice of local counsel on the criteria or qualifications for obtaining such licenses should be sought.

However, from a general standpoint, the criteria for obtaining each license shall be based on the following qualifications of the applicants:

- nationality
- types of entity
- registered and paid-up capital
- objectives of the company
- board composition
- directors and major shareholders qualifications
What are the licenses required and what are the criteria and process involved?

The licenses required will depend on the specific activities contemplated. We recommend seeking the advice of local counsel.

For banking, lending, payment, foreign exchange–related services, licenses or approvals are required by the SBV. For instance, to provide intermediary payment services (for example, e-wallet, payment portal), fintech/insurtech companies must apply for an intermediary payment license at the SBV.

For insurance businesses, insurers and insurance brokers are required to apply for a business license from the MOF’s Insurance Supervisory Authority.

For securities and fund management businesses, licenses or approvals are required by the MOF’s State Securities Commission.

Furthermore, if the fintech/insurtech innovation involves a patentable invention or if there are plans to register a trademark, the relevant companies are strongly recommended to obtain the patent and/or trademark registrations.

Criteria to obtain a license and how long it takes to obtain the license depend on the type of license to be applied, the relevant laws and the licensing authorities.

From a general standpoint, the criteria to obtain licenses shall be based on legal conditions under local laws and relevant international treaties, for example, Vietnam’s WTO Commitments, financial capacity of investors, requirements and feasibility of proposed business models, registered and paid-up charter capital, corporate governance requirements, and requirements on key personnel and human resources. The timeline may also vary depending on whether the direct licensing authority needs to consult with higher or relevant authorities before it issues the license.
<table>
<thead>
<tr>
<th>Country</th>
<th>Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>There are no specific regulations for the use of biometrics on its own. Biometric data is regulated by the Privacy Act 1988 (Cth). The Australian Law Reform Commission (ALRC) has also recently recommended that certain biometric information be labelled as sensitive information to afford consumers greater protection. The Intelligent Access Program (IAP), is a national program developed in partnership with all Australian road agencies, and is the first road regulatory use of telematics in Australia. The IAP relies on certified telematics providers (IAP service providers) and their approved GPS-based telematics devices and systems (approved intelligent transport systems) to offer road authorities a compliance solution when it comes to allowing operators of certain vehicles access or enhanced access to the public road network.</td>
</tr>
<tr>
<td>China</td>
<td>Provision of telematics services is regulated in China. Specifically, location-based information services are subject to licensing and regulatory requirements for the providing Internet mapping services and value-added telecommunications services in China. Use of biometrics data is not specifically regulated under Chinese law.</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>The PCPD has issued the &quot;Guidance on Collection and Use of Biometric Data&quot; and indicated that biometric data (for example, physiological data and behavioral data) can be considered as personal data under the Personal Data (Privacy) Ordinance (Cap. 486). Accordingly, insurers and insurance intermediaries collecting or using biometric data could be regarded as data users under the ordinance and such data should only be used where justified. Appropriate procedural and technological safeguards should also be put in place to prevent unauthorized access to and wrongful use of biometric data. Insurers and insurance intermediaries should ensure that such use is compliant with any existing regulations or conduct of business requirements. Further, depending on how such technology is used, we may need to consider whether other areas of regulation are attracted.</td>
</tr>
<tr>
<td>Indonesia</td>
<td>There is no regulation regarding telematics and biometrics in Indonesia. The utilization of telematics and biometrics in Indonesia itself is still relatively rare. In relation to personal data used in biometrics, under MOCI regulation the use, broadly defined, of any data analytic activities using customers' personal data must have received a specific consent from the data owner/customer.</td>
</tr>
<tr>
<td>Country</td>
<td>Regulations for Telematics and Biometrics</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Japan</td>
<td>There are no specific regulations for the use of telematics. However, any insurance product that uses the telematics must ensure that the use is compliant with any existing insurance regulations such as approval for new insurance products. In relation to the use of biometrics, the Guidelines for Personal Information Protection in the Financial Sector (Personal Information Protection Guidelines) impose stringent restrictions on the collection, use and transfer of sensitive personal information in addition to the restrictions to be generally applied to the collection, use and transfer of any personal information under the APPI. Although the collection, use and transfer of sensitive personal information are generally prohibited under the Personal Information Protection Guidelines, the collection, use and transfer of biometrics, falling under the category of sensitive personal information for the purpose of identity verification, are permitted exceptions, subject to consent of the data subject. Under the Personal Information Protection Guidelines, financial institutions must, in particular, carefully handle sensitive personal information to avoid any collection, use and transfer deviating from the purpose mentioned above. The Practical Guidelines for Security Control Measures provided in the Guidelines for Personal Information Protection in the Financial Sector (Practical Guidelines) further set out the detailed measures that need to be taken in relation to biometrics falling under the category of sensitive personal information.</td>
</tr>
<tr>
<td>Malaysia</td>
<td>There are no specific regulations for the use of telematics or biometrics. It is likely that insurers will continue to be subject to general conduct of business and data privacy requirements. Further, depending on how such technology is used, other areas of regulation (for example, telecommunications or pharmaceuticals) may apply.</td>
</tr>
<tr>
<td>Myanmar</td>
<td>There are no specific regulations for telematics or biometrics. Further, there are no provisions regarding data privacy in Myanmar. Where the insurer operates any financial elements of its business in Myanmar, however, it may be captured by the duty of secrecy which is required under the Financial Institutions Law 2016.</td>
</tr>
<tr>
<td>Philippines</td>
<td>There are no specific regulations for the use of telematics or biometrics on its own. However, the processing of personal information attached to the telematics or biometrics will attract data privacy implications under the DPA. Further, depending on how such technology is used, we may need to consider whether other areas of regulation are attracted (for example, telecommunications or pharmaceuticals).</td>
</tr>
<tr>
<td>Singapore</td>
<td>There are no specific regulations for the use of telematics or biometrics on its own; however, insurance companies should ensure that such use is compliant with any existing regulations or conduct of business requirements. Data privacy concerns will also apply. Further, depending on how such technology is used, we may need to consider whether other areas of regulation are attracted (for example, telecommunications or pharmaceuticals).</td>
</tr>
</tbody>
</table>
Is the use of telematics and/or biometrics regulated?

<table>
<thead>
<tr>
<th>Country</th>
<th>Regulations and Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAIWAN</td>
<td>Except for the Personal Data Protection Act, there are no specific regulations for the use of telematics or biometrics on its own. Insurance companies should ensure that such use is compliant with any existing regulations or conduct of business requirements.</td>
</tr>
<tr>
<td>THAILAND</td>
<td>There are no specific regulations for the use of telematics or biometrics on its own; however, insurance companies should ensure that such use is compliant with any existing regulations or conduct of business requirements. Further, depending on how such technology is used, we may need to consider whether other areas of regulation are attracted (for example, telecommunications or pharmaceuticals). In addition, if any insurance company engages in an electronic transaction, such insurance company shall be subject to the Secure Method Royal Decree issued under the Electronic Transactions Act (the E-Transactions Act), which requires an application of information technology security at a strict level.</td>
</tr>
<tr>
<td>VIETNAM</td>
<td>There are no specific regulations for the use of telematics or biometrics on its own. However, insurance companies should ensure that such use is compliant with any existing regulations or conduct of business requirements. Data privacy concerns may also apply. Further, depending on how such technology is used, we may need to consider whether other areas of regulation are attracted (for example, telecommunications or pharmaceuticals).</td>
</tr>
</tbody>
</table>
### AUSTRALIA

There is no specific regulation drawing a distinction between institutions that are "too big to fail" versus "too small to care."

However, as big institutions carry higher risks to the relevant financial systems, and any failures or non-compliance can significantly impact market or investor confidence, they often receive closer attention from the relevant authorities. On the other hand, new emerging fintech/insurtech companies enjoy certain regulatory exceptions (as discussed above) in circumstances where they represent a limited prudential and lower level of consumer risk.

### CHINA

No.

### HONG KONG

There can be different standards of regulation for retail payment systems. Under the Payment Systems and Stored Value Facilities Ordinance (Cap. 584), the HKMA administers a designation system for retail payment systems (RPS), and may designate an RPS if it considers that the system is likely to become an RPS whose proper functioning is material to the monetary or financial stability of Hong Kong. A designated RPS is required to comply with the control and compliance requirements under the ordinance.

### INDONESIA

Not for fintech/insurtech at the moment (and this is relevant currently only for banks). Although there is no regulation that specifically regulates fintech/insurtech activities, the OJK appreciates that there may be a changing risk profile and proposed regulation will address the risk from fintech/insurtech innovation. However, regulation will be proportional to the risks associated with the relevant fintech/insurtech activities.

### JAPAN

Based on the discussions in the Study Group and the FinTech Review Committee, drawing a clear distinction between institutions that are "too big to fail" and "too small to care" has not been a big focus. However, some regulations contain aspects such as the Payment Services Act, which defines fund transfer service as transfer of a certain limited fund (JPY1 million under the subordinate regulations) or less, whereas any fund transfer of a larger amount is supposed to be handled by licensed banks. The PPC and FSA Guidelines mention 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 required not 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 transfer of Sensitive Data.
### Malaysia
Yes, both BNM and the SC have indicated that different markets are subject to different levels of regulation, that is, adopting the concept of proportionate regulation. By way of examples:

- The SC takes the position that “the level of regulation imposed will depend on the proposed market characteristics, including the structure of the market; sophistication of market users and rights of access; types of products traded; and risks posed by such markets” for operators of equity crowdfunding.
- The CMSA distinguishes between the levels of investor protection for institutional and non-institutional investors.
- The FSA distinguishes payment systems and designated payment systems, which could affect public confidence or impact monetary stability and therefore carry a higher risk than normal payment systems.

### Myanmar
No.

### Philippines
Yes, some banks in the Philippines are tagged as "too big to fail" or "D-SIB" (for domestic systemically important banks). D-SIBs are characterized as banks whose distress or disorderly failure would cause significant disruptions to the wider financial system and economy. A bank's classification as a D-SIB is based on four criteria: size, interconnectedness, substitutability and complexity.

Higher capital requirements are imposed on banks identified as a D-SIB. Furthermore, D-SIBs are subject to higher supervisory expectations by the BSP.

Furthermore, IPOPHL fees for IP services vary for big entities vis-à-vis small entities.

With respect to capital markets participants, the SEC does not make such a distinction.

### Singapore
Yes, there can be different standards of regulation, for example, for payment systems. While the MAS has general oversight functions and information-gathering powers over payment systems, it has more extensive powers in relation to designated payment systems, which are those where the MAS is satisfied that a disruption in the operations of the payment system could trigger, cause or transmit further disruption to participants or systemic disruption to the financial system of Singapore; a disruption in the operations of the payment system could affect public confidence in payment systems or the financial system of Singapore; or it is otherwise in the interests of the public to do so.

Based on recent public announcements by the MAS, this distinction between "too big to fail" and "too small to care" may also be applied to fintech/insurtech innovations that may not already be regulated. This is because, as mentioned, the MAS has announced that it will apply a materiality and proportionality test and regulation introduced to address risks from fintech/insurtech innovation must be proportionate to the risk posed.
<table>
<thead>
<tr>
<th>Country</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taiwan</td>
<td>Yes, there can be different standards of regulation. For example, under the Electronic Payment Institutions Act, if the daily balance of the funds in the third-party payment service provider's account during the past one-year period does not exceed NTD 1 billion (approximately USD 303 million), such service provider is not required to obtain an electronic payment institution license from the FSC.</td>
</tr>
<tr>
<td>Thailand</td>
<td>Currently, there is no specific distinction between institutions that are &quot;too big to fail&quot; versus &quot;too small to care.&quot; Distinction is drawn based on types of entity and types of businesses that such entity is engaged in.</td>
</tr>
<tr>
<td>Vietnam</td>
<td>There is no specific legal regulation drawing a distinction between institutions that are &quot;too big to fail&quot; versus &quot;too small to care.&quot; However, in practice, large-scale institutions or entities carrying higher risks to the relevant financial systems, whether or not from fintech/insurtech innovation, often receive more attention from or stricter supervisions by the authorities.</td>
</tr>
</tbody>
</table>
What laws (if any) do insurance companies have to comply with in respect of technology risk management?

### Australia

While not a strict legal requirement, APRA has released Practice Guides on the management of security risk in information and information technology that is applicable to insurance companies. Topics addressed include: the importance of an overarching framework, systematic IT asset life-cycle management, effective monitoring processes and robust IT security reporting and assurance mechanisms.

OAIC guidelines and APRA Prudential Practice Guides also indicate the importance of adequate disaster recovery processes as part of an organization’s robust IT, cybersecurity and management systems.

From a personal data privacy perspective, insurance companies 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 insurance company that holds personal information must:

- 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

According to the Guidelines for the Administration over the Informatization of Insurance Companies (for Trial Implementation) issued by CIRC, effective 1 January 2010, insurance companies established and licensed within China are required to comply with the following obligations with respect to technology risk management:

- establish data center and disaster recovery center within the territory of China
- establish and implement detailed internal rules and systems concerning IT and network security management
- appoint a chief information officer or a person who is mainly responsible for the IT-related work
- conduct security assessment before implementation of new information systems and/or technologies
- establish monitoring and reporting system for IT security
- conduct risk assessment and audit of IT system
### What laws (if any) do insurance companies have to comply with in respect of technology risk management?

<table>
<thead>
<tr>
<th>Country</th>
<th>Regulations and Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HONG KONG</strong></td>
<td>The IA has published the “Guideline on the Use of Internet for Insurance Activities” (GL 8), which applies to authorized insurers and insurance intermediaries in relation to their insurance activities or transactions conducted on the Internet. GL 8 requires all practicable steps to be taken to ensure that a comprehensive set of security policies and measures that keep up with the advancement in Internet security technologies shall be in place and that the electronic payment system (for example, credit card payment system) shall be secure. Also, based on the IA’s “Guideline Note on the Corporate Governance of Authorized Insurers” (GL10), from a corporate governance perspective, the boards of certain authorized insurers shall ensure that there are in place a sound internal control system and a comprehensive risk management policy. From a data privacy perspective, insurers and insurance intermediaries should take appropriate measures to protect the customer data against unauthorized or accidental access, processing or erasure. The PCPD has also issued the “Best Practice Guide for Mobile App Development,” which provides guidance on how data privacy protection measures should be incorporated into the development process of a mobile app.</td>
</tr>
<tr>
<td><strong>INDONESIA</strong></td>
<td>There are no specific laws and regulations in the insurance sector prescribing rules on technology risk management. The existing regulations are more general in nature, old school and are principle-based regulations (rather than regulations that clearly set out relevant requirements). Given the absence of clear requirements, businesses need to be prudent, take security steps, do due diligence and ensure that internal control systems are properly implemented.</td>
</tr>
<tr>
<td><strong>JAPAN</strong></td>
<td>The Insurance Supervision Guidelines contain the provisions regarding system risk management environment as one of the points to be assessed to examine the appropriateness of insurance companies' operational risk management environment.</td>
</tr>
<tr>
<td><strong>MALAYSIA</strong></td>
<td>Among others, licensed insurers must comply with the Guidelines on Management of IT Environment and Guidelines on Data Management and MIS Framework issued by BNM. Licensed insurers that carry out Internet insurance activities must also comply with BNM’s Guidelines on Internet Insurance (Consolidated) issued by BNM. The Guidelines on Risk Governance and Guidelines on Stress Testing and the Code of Conduct for Malaysia Wholesale Financial Markets, both of which extend to the use of technology, also apply. There is also a reporting and/or notification requirement on insurers in the event of cybersecurity breaches and cyber threats.</td>
</tr>
<tr>
<td><strong>MYANMAR</strong></td>
<td>There are no specific laws and regulations in the insurance sector prescribing rules on technology risk management. The existing regulations focus more generally on ensuring that there are sufficient funds provided by all insurers to have capacity to provide insurance repayments when or if required.</td>
</tr>
</tbody>
</table>
### What laws (if any) do insurance companies have to comply with in respect of technology risk management?

<table>
<thead>
<tr>
<th>Region</th>
<th>Regulations and Compliance Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PHILIPPINES</strong></td>
<td>Insurance companies should comply with the Guidelines on Electronic Commerce of Insurance Products issued by the Insurance Commissioner. The guidelines provide for online privacy requirements and security of payment and personal information, among others. Department Circular No. 2017-002, issued by the Department of Information and Communications Technology, prescribes the use of cloud computing technology for all government agencies. The Circular contains guidelines on developing security frameworks according to a government agency’s specific needs and the type of data being handled. In addition, the Philippines’ Data Privacy Act of 2012 (DPA), its implementing rules and regulations, and the related issuances of the National Privacy Commission (NPC) regulate the processing of personal data. The DPA requires all personal data processors and controllers to implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data.</td>
</tr>
<tr>
<td><strong>SINGAPORE</strong></td>
<td>Licensed insurers (other than captive insurers and marine mutual insurers) will need to comply with MAS 127 Notice on Technology Risk Management, registered insurance brokers will need to comply with Insurance companies MAS 506 Notice on Technology Risk Management, and licensed financial advisers will need to comply with FAA-N18 Notice on Technology Risk Management. The Technology Risk Management Guidelines, Business Continuity Guidelines, MAS 126 Notice Enterprise Risk Management for Insurers, MAS Circular No. SRD TR 02/2014 IT Security Risks Posed By Personal Mobile Devices, MAS Circular No. SRD TR 01/2014 System Vulnerability Assessments and Penetration Testing, MAS Circular No. SRD TR 01/2015 Early Detection of Cyber Intrusions and MAS Circular No. SRD TR 03/2015 Technology Risk and Cyber Security Training for Board will also need to be complied with.</td>
</tr>
<tr>
<td><strong>TAIWAN</strong></td>
<td>According to the Guidelines for Insurance Enterprise to Conduct Electronic Commerce promulgated by FSC, an insurer licensed to conduct e-commerce shall obtain the international standard verification of information security management system (ISO27001) by 1 July 2017. If the insurer fails to obtain and maintain the ISO27001 verification before the deadline, it will be prohibited from operating the e-commerce business. In addition, the licensed insurer shall also comply with the Guideline for Life Insurance Enterprises to Conduct Security Assessments on Computer System/Information Security and the Guideline for Non-Life Insurance Enterprises to Conduct Security Assessments on Computer System/Information Security to conduct the technology risk assessment and management.</td>
</tr>
</tbody>
</table>
## What laws (if any) do insurance companies have to comply with in respect of technology risk management?

**THAILAND**

Licensed insurers will need to comply with the OIC Notification re: Criteria, Processes and Conditions in Prescribing Minimum Standard for Risk Management of Life Insurance Companies B.E. 2560 (2017) and OIC Notification re: Criteria, Processes and Conditions in Prescribing Minimum Standard for Risk Management of Non-Life Insurance Companies B.E. 2560 (2017). These new notifications have adopted the concept of enterprise risk management in accordance with the international standard of International Association of Insurance Supervisors (IAIS) and a number of new requirements, for example, establishment of risk management committee, preparation of frameworks, and reporting requirements. The notifications have been announced by the OIC and are expected to be published in the Royal Gazette by September 2017 and come into force 180 days thereafter.

As mentioned in the response to question 3, the Secure Method Royal Decree requires insurance companies that engage in e-transaction to apply the required information technology security at a strict level and to comply with the security method management stipulated therein.

If any insurance company offers an e-payment service to customers and if it is regarded as an e-payment service provider under the E-Transactions Act, it is required to comply with security methods applicable to e-payment service providers under the Bank of Thailand Notification No. SorRorKor 3/2552 Re: Policies and Measures on Security of Information Systems for Business Operations of Electronic Payment Service Providers.

---

**VIETNAM**

Insurance companies should comply with the Information Technology Law, the Law on Network Information Security, and the Law on E-Commerce and relevant specific guiding regulations.
The Privacy Act 1998 (Cth) governs the collection, use, storage, disclosure and transfer of personal data. The Privacy Act applies to companies with an annual turnover of more than AUD 3 million (APP entity).

An APP entity 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 an 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.
Are there any laws governing big data, including the collection, use, storage, disclosure and transfer of personal data?

**CHINA**

There is no comprehensive personal data protection law in China, but the concept exists under various laws and regulations such as the Tort Liability Law, the Criminal Law, the NPC Decision on Strengthening the Protection of Network Information and the Consumer Protection Law.

In the context of collecting and processing electronic personal data, the relevant Chinese laws and regulations require that organizations must expressly inform the data subjects the purposes, scope and manner of data collection and use and obtain their consent to the same. Furthermore, organizations have an obligation to (i) keep the personal data of data subjects confidential, and must not disclose (unless with the data subject’s consent), sell or unlawfully provide the same to a third party, and (ii) adopt technical and other necessary measures to ensure that the data is secure, and must take remedial steps immediately where data disclosure, damage or loss occurs or may occur.

Chinese central government has shown increased interest in the use of big data by issuing several notices and circulars with framework policies and rules dealing with storage and use of big data by government agencies. Detailed enabling rules or specific regulations to govern the use of big data is yet to be promulgated.

**HONG KONG**

The Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO**) applies to the private sector as well as the public sector. The PDPO regulates the collection, use, storage, disclosure and transfer of personal data in Hong Kong. In addition to the baseline requirements of the PDPO, the PCPD has issued guidance and published commentaries related to collection of personal data through the internet and online behavioral tracking.

Insurance companies may also need to ensure that their dealing with personal data does not contravene any business conduct requirements. For example, under the proposed new regulatory regime for insurance intermediaries (which will be administered by the Insurance Authority), there are conduct requirements requiring an insurance intermediary to act honestly, fairly, in the best interests of the policyholders (or the potential policyholders), and with integrity, and to ensure that the assets of the policyholders (or the potential policyholders) are promptly and properly accounted for.
Are there any laws governing big data, including the collection, use, storage, disclosure and transfer of personal data?

**INDONESIA**

Indonesia does not have a regulation that deals specifically with big data. There are several regulations that govern the transfer of data or data storage:

**Transfer of data**

Under Article 1 (27) of Regulation 82, private data means any individual data the validity of which is saved, maintained and kept, and the confidentiality of which is to be protected. As the EIT Law and Regulation 82 regulates electronic transactions, they only regulate data protection issues related to electronic transactions, and the term private data under the EIT Law is defined strictly as individual data that is saved, maintained or kept in the form of electronic data.

Under Article 15 of Regulation 82, the administrator of an Electronic System (Penyelenggara Sistem Elektronik) is obliged to:

- maintain the confidentiality, unity and availability of private data
- secure that the collection, use and utilization of private data is done upon the consent of the owner of private data, unless provided otherwise by applicable laws and regulations
- secure that the use or disclosure of data is conducted with the consent of the owner of private data and in accordance with the purpose conveyed to him/her at the time of collection of the private data.

However, Regulation 82 and the EIT Law do not provide clear definitions of the terms "collection," "use" and "utilization" of private data. Therefore, the terms can be interpreted in a general manner.

The EIT Law and Regulation 82 do not clearly define "owner of private data." As a result, the definition of the owner of private data can be broadly interpreted (for example, an individual, Indonesian or foreign citizen, legal entities, etc.).

POJK 1 and Circular Letter No 14/SEOJK.07/2014 on Confidentiality and Security of Consumers' Private Information and/or Data provides that financial services companies that obtain personal data from third parties (including individuals and entities) and intend to use that data must obtain written statements from those third parties that those third parties have obtained written approval from their consumers consenting to the use of that data. Any transfer of consumers' data to any third party can be done only with prior written consent from the consumers, and when the financial services companies transfer these data to any third parties (based on the consumers' written consent), the financial services companies must ensure that the third parties receiving the data will only use the data for the agreed purpose. Circular 14 further provides that consumer personal information includes the following data: (i) for individual consumers: name, address, date of birth and age, telephone number and name of birth mother; and (ii) for corporate consumers: name of company, address, composition of directors and commissioners, including data of their identification documents such as passports, KTP or stay permits; and shareholders composition.

POJK 1 provides that consent from customers on the use of their data (including to transfer the data) must be obtained in writing.
Are there any laws governing big data, including the collection, use, storage, disclosure and transfer of personal data?

Data storage

GR 82 requires all electronic system operators for "public service" to have their data center and disaster recovery center onshore by October 2017. Under the EIT Law, an "electronic system operator" is defined as any person, state entity, business entity and community that provides, manages and/or operates an electronic system whether independently or collectively to an electronic system user for its own use and/or another party’s use. Based on the above definitions (which are broad in nature), any person or entity that manages and operates electronic systems (such as websites, applications, email and messenger), and provides those systems to other parties, may be considered as an electronic system operator. Bank Indonesia BI Regulation 9/2007 specifically requires the data center and disaster recovery center for banks to be located onshore. BI Regulation 9/2007 stipulates that if a bank intends to have its data center and/or disaster recovery center offshore, it must first obtain a prior approval from Bank Indonesia and/or OJK and comply with certain requirements (as further explained below). BI Regulation 9/2007 also provides that banks may only engage an offshore third-party IT service provider with Bank Indonesia and/or OJK's prior approval.

Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic System (Data Protection Regulation) requires any use, which is broadly defined, of personal data, through an electronic system, may only be done with the prior consent from the data owner. The consent must be in writing (meaning an express consent), whether manually or electronically, and in the Indonesian language (although there is no prohibition in using a dual language consent, so that format can be used, if preferred). Further, the consent is only effective if the electronic system operator has given an explanation on the specific intended use of the personal data.

The OJK issued a new regulation in December 2016 that requires, before October 2017, all insurance companies to localize their data centers and disaster recovery centers in Indonesia for the following customer data:

- Data and information related to the personal data of the policyholder, the insured, or participants (name, address, date of birth, etc.)
- Data and information relating to premium payments or claims
- Data and information on the nationality (national ID number or passport details)
- Data and information on the relevant legal entities (tax file number of participants, business license registration number, etc.)

JAPAN

The APPI applies to business operators handling personal information database. The APPI regulates the collection, use, storage, disclosure and transfer of personal data. However, there were discussions that it was unclear whether big data would fall under the category of personal information and accordingly whether the APPI would apply. Under the amended APPI promulgated on 30 May 2017 (Amended APPI), the definition of personal information is expanded and it is clarified that anonymized and unrestorable personal information can be used under certain relaxed requirements.

In addition to the baseline requirements of the APPI, additional specific requirements under the Personal Information Protection Guidelines will apply to financial institutions, including insurance companies.
<table>
<thead>
<tr>
<th>Country</th>
<th>Description</th>
</tr>
</thead>
</table>
| Malaysia | The Malaysian Personal Data Protection Act 2010 (PDPA) governs personal data collected or processed in respect of commercial transactions by persons established in Malaysia or who use equipment in Malaysia to process personal data. In addition to the baseline requirements of the PDPA, additional requirements apply with respect to sensitive personal data (such as medical records, political affiliations and others) and data users in prescribed industries (such as the medical, banking and insurance industries).

The PDPA sets out data protection principles governing the collection, use, disclosure, accuracy, retention, access to and security of personal data. Data users are also required to develop and implement a security policy that complies with prescribed security standards. Insurers are also required to comply with the Code of Practice on Personal Data Protection for the Insurance and Takaful Industry in Malaysia issued pursuant to the PDPA effective on 23 December 2016 (Relevant Code of Practice).

The FSA and CMSA also have specific confidentiality restrictions relating to regulatory-related information and customer information. |
| Myanmar | There are no general data privacy laws.

There are specific confidentiality and secrecy requirements in some industries (for example, banking and telecommunications); however, these will not apply to insurance companies unless they also operate in those industries. More likely, confidentiality requirements are contained in the specific insurance licenses granted by the Insurance Business Supervisory Board. |
| Philippines | Insurance companies should comply with the Guidelines on Electronic Commerce of Insurance Products issued by the Insurance Commissioner. The guidelines provide for online privacy requirements and security of payment and personal information, among others.

In addition, the Philippines’ Data Privacy Act of 2012 (DPA), its implementing rules and regulations, and the related issuances of the National Privacy Commission (NPC) regulate the processing of personal data. “Processing” of personal data is defined under the DPA as “any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.”

Personal data, as it is defined under the DPA, may refer to any of the following:

- Personal information, which refers to “any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.”

- Sensitive personal information, which refers to personal information: (a) about an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (b) about an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (c) issued by government agencies peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (d) specifically established by an executive order or an act of Congress to be kept classified. |
The principal requirement under the DPA for the processing of personal data is the consent of the data subject. As a general rule, the consent of the data subject to the processing of his or her personal data is required, and must be evidenced by written, electronic or recorded means. If personal data is intended to be shared or transferred to third parties, service providers or other data processors, the data subject’s specific consent to such data sharing would also be required. The timing of the consent would vary depending on the type of information involved in the processing. If the information pertains to simply personal information, then consent must be procured prior to the collection, or as soon as practicable and reasonable. On the other hand, with respect to the processing of sensitive personal information, the DPA exacts a stricter standard: the data subject’s consent at all times must be procured prior to the processing of the sensitive personal information.

Singapore's Personal Data Protection Act 2012 (PDPA) and its attendant Personal Data Protection Regulations (which came into effect on 2 July 2014) applies to all organizations in the private sector. The PDPA regulates the collection, use, storage, disclosure and transfer of personal data in Singapore. In addition to the baseline requirements of the PDPA, additional specific mandatory regulations also apply to certain industries (such as banking and medical) with respect to certain categories of sensitive personal data (such as bank customer information and medical records).

The Personal Data Protection Commission (PDPC) has issued advisory guidelines, which indicate the manner in which the PDPC will interpret provisions of the PDPA. Of interest to insurance companies and fintech/insurtech businesses seeking to utilize big data and telematics are the advisory guidelines on the PDPA for selected topics such as analytics and research, and on anonymization, which was revised on 28 March 2017. There are also industry-led guidelines developed by the insurance industry associations, such as the LIA Code of Practice for Life Insurers on the PDPA, and the LIA Code of Conduct for Tied Agents of Life Insurers on the PDPA.

In addition, the PDPC recently, on 20 January 2017, introduced and updated its advisory guidelines to help companies better protect personal data in compliance with the PDPA. The new and/or updated guidelines include:

(a) Guide to preventing accidental disclosure when processing and sending Personal Data (new)
(b) Guide to securing Personal Data in electronic medium (updated)
(c) Guide to disposal of Personal Data on physical medium (updated)
(d) Guide on building websites for SME (updated)

Insurance companies will also need to ensure that their dealing with personal data do not contravene any business conduct requirements or any technology risk management guidelines.
| TAIWAN | Taiwan's Personal Data Protection Act (amended on 30 December 2014) (TPDPA) and relevant regulations and rulings apply to government authorities, all organizations in the private sector and individuals. The TPDPA regulates the collection, use, process and cross-border transfer of personal data in Taiwan.

The TPDPA provides the definition for "use," "process" and "cross-border transfer." "Process" means in order to establish or use the personal data, to record, input, storage, edit, correct, duplicate, index, delete, output, link or transfer for internal use the personal data. "Use" means to use the collected personal data in ways other than the "use." "Cross-border transfer" means to process or use the data subject across border.

The Insurance Act of Taiwan regulates the collection and use of sensitive personal data. Under the Insurance Act, the following person/entity may collect, process or use sensitive personal data (medical records, medical treatment or health examination of individuals), with the written consent of the data subject:

(a) insurance enterprises, insurance agents, brokers and surveyors that operate or conduct business in accordance with the Insurance Act

(b) juristic persons commissioned by insurance enterprises to provide assistance in confirming or performing their obligations under an insurance contract

(c) insurance-related foundations established with the permission of the competent authority to handle disputes and matters relating to compensation for victims of motor vehicle accidents |

| THAILAND | There is currently no specific law governing big data. Exploitation of personal data may be done without the consent of the data subject if that use does not unlawfully injure the personal data rights of the data subject. However, any use of personal data in a way that unlawfully injures the right to personal data, intentionally or negligently, would violate the Constitution and may constitute a wrongful act (a tort) under the Thai Civil and Commercial Code.

In addition, the use of personal data by certain types of business sector is regulated under specific laws, such as telecommunications, credit bureau or financial services.

If an insurance company offers an e-payment service to customers and if it is regarded as an e-payment service provider under the E-Transactions Act, it is required to stipulate a personal data policy (that is, user data retention and confidentiality level).

The Thai Cabinet approved in principle the Personal Data Protection Bill (the PDPB) in January 2015. It is pending further consideration by relevant authorities before passing into law. The PDPB has certain restrictions with regard to the collection, use, storage, disclosure and transfer of personal data. For example, consent must be obtained from the data owners for the collection, use, and disclosure of personal data. The transfer of personal data is subject to certain conditions unless the consent is obtained from data owners for the transfer. If the PDPB enters into force, insurance companies would be subject to the requirements under the PDPB.

Please note, however, that there is no specific timeline when the PDPB will be passed and it is still subject to changes. |
| **8.** Are there any laws governing big data, including the collection, use, storage, disclosure and transfer of personal data? |

| **VIETNAM** | Vietnam has no single comprehensive law that governs big data or addresses individual and organizational privacy rights. Instead, these issues and relevant provisions are governed under the Civil Code, the IT Law, the Law on Network Information Security, the Consumer Protection Law, the Penal Code, the Insurance Business Law, the Telecommunications Law and other specialized regulations (where applicable), where these matters are addressed in fairly general terms, and in certain implementing regulations that contain more specific provisions. |
9 Are there any restrictions that could hinder the growth and usage of insurtech by insurance companies under data privacy laws?

<table>
<thead>
<tr>
<th>Country</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUSTRALIA</td>
<td>To the extent that the insurance company has an annual turnover of more than AUD 3 million per year, its activities and usage of insurtech remains subject to the Privacy Act and the requirements of the APPs as set out in response to question 3(a) above.</td>
</tr>
<tr>
<td>CHINA</td>
<td>No.</td>
</tr>
</tbody>
</table>
| HONG KONG | Yes, the PDPO provides that:  
  - a data user needs to take practical steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use  
  - personal data must be accurate and should not be kept for a period longer than is necessary to fulfill the purpose for which it is used  
  - personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject |
| INDONESIA| No. However there is an express requirement to obtain written specific consent from customers before transferring data. Businesses need to consider the most practical way to obtain the written consent from customers. In practice, insurance companies include the consent in their standard insurance policy clause. Given the Data Protection Regulation (fully effective in December 2018), insurance companies must refine their consent language to conform with the Data Protection Regulation. Before the Data Protection Regulation was enacted, consent language could be very broad and general (for example, a blanket approval). Now consents must be very specific. For example, the customer must know and specifically consent to the actual use of that data (such as data analytics). |
| JAPAN     | With respect to transfer of personal information, under the APPI, there were no specific provisions regulating the transfer of personal information to third parties who are located overseas and it was unclear whether the APPI would apply to such third parties. Under the Amended APPI, in order to transfer personal information to third parties who are located overseas, unless (i) such third parties are located in countries that have personal information protection system comparable to that of Japan or (ii) such third parties establish the system that meets the requirements necessary to continuously take measures corresponding to requirements under the Amended APPI, the transferor needs to obtain the data subject's consent to transfer to third parties who are located overseas.  
  With respect to big data, as discussed above, under the APPI, there were discussions whether the APPI would apply to the use of big data and therefore the relevant market players, including insurance companies, tended to hesitate to use big data. Under the Amended APPI, the Guidelines for the Act on Protection of Personal Information (Edition of Anonymously Processed Information) clarified to what extent the business operators need to have personal information anonymized in order for the information to be treated as anonymized data, which can enjoy the benefit of the relaxed requirements.  
  Although it is not specifically related to the insurance sector, the Japan Fair Trade Commission has an awareness of the issue about domination of big data by large companies. It published the report of its study group, the Review Committee of Data and Competition Policy, on 6 June 2017. The report mentioned the possibility of application of the Anti-Monopoly Act for certain activities such as unfair data collection or data hoarding. |
Are there any restrictions that could hinder the growth and usage of insurtech by insurance companies under data privacy laws?

<table>
<thead>
<tr>
<th>Country</th>
<th>Regulations and Compliance Requirements</th>
</tr>
</thead>
</table>
| Malaysia    | The PDPA and the Relevant Code of Practice provide certain requirements in relation to the processing of personal data. Some of the requirements under the PDPA are as follows:  
  - Consent from the data subject is required prior to the personal data being processed (including a transfer of such personal data)  
  - A written notice must be issued to notify the data subject of a prescribed list of information in the Malay and English languages  
  - The personal data shall not be disclosed for any purpose other than the purpose for which it is disclosed  
  - A data user shall take practical steps to protect the personal data  
  - The personal data processed shall not be kept longer than is necessary  
  - A data user must take all reasonable steps to ensure that the personal data is, among others, accurate and not misleading  
  - A data subject must be provided access to his personal data and be able to correct his personal data. |
| Myanmar     | Not specifically arising from data privacy laws.                                                      |
| Philippines | Yes. The DPA imposes stringent compliance obligations on persons or entities engaged in the processing of personal data. For instance, under the DPA, personal information controllers and processors shall have the following responsibilities:  
  - Ensure that proper safeguards are in place to guarantee the confidentiality of the personal information processed and prevent its use for unauthorized purposes  
  - Implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing  
  - Use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party  
  - Designate an individual, called a data protection officer, who is accountable for the entity’s compliance with the DPA.  
Furthermore, the DPA mandates the registration of processing systems of personal information controllers and processors that are involved in the processing of sensitive personal information of at least 1,000 individuals, whether it be of employees, clients, customers or contractors. The current deadline for this registration requirement is on 9 September 2017. Note that failure to comply with the DPA may mean not only mandatory business closure for the controller and processor but also payment of damages and of steep fines. For responsible officers and employees, non-compliance by their organizations may even result to imprisonment. |
### Are there any restrictions that could hinder the growth and usage of insurtech by insurance companies under data privacy laws?

<table>
<thead>
<tr>
<th>Country</th>
<th>Restrictions and Compliance Requirements</th>
</tr>
</thead>
</table>
| **Philippines** | Moreover, an obscure law, Presidential Decree No. 1718, passed in 1980, prohibits the transfer of documents or information relating in any manner to any business carried on in the Philippines, unless the sending thereof complies with the following:  
- consistent with and forms part of a regular practice of furnishing to a head office or parent company or organization outside of the Philippines  
- in connection with a proposed business transaction requiring the furnishing of the document or information  
- required or necessary for negotiations or conclusions of business transactions, or is in compliance with an international agreement to which the Philippines is a party  
- made pursuant to the authority granted by the designated representative of the President of the Philippines  
While Presidential Decree No. 1718 has not been strictly enforced, it nevertheless imposes criminal penalties for violations thereof. |
| **Singapore** | Yes, the PDPA provides the following:  
- an organization (including insurance companies) should not transfer personal data outside of Singapore unless it ensures that the transferred personal data will be afforded a standard of protection that is at least comparable to that provided under the PDPA  
- an organization is required to ensure that personal data in its possession and control is protected from unauthorized access and use, and implement appropriate physical, technical and organizational security safeguards commensurate with the amount, nature and sensitivity of the personal data involved, to protect the personal data  
- an organization should cease to retain personal data as soon as it is reasonable to assume that the purpose for which the personal data was collected is no longer being served and when the retention is no longer necessary for legal or other business purposes |
| **Taiwan** | Yes. According to the TPDPA, the Taiwan government may prohibit an individual/entity from conducting cross-border transfer of the personal data under one of the following circumstances:  
- where substantial national interests are involved  
- where international treaties or agreements specify otherwise  
- where the rights and interests of the data subject are likely to be damaged as a result that the data recipient country does not have appropriate laws and regulations to protect personal data  
- where the TPDPA may be avoided because the personal data is transmitted or used by way of indirect transmissions to a third country or area  
In addition, according to the Directions for Operation Outsourcing by Insurance Enterprises, an insurance enterprise shall obtain the FSC’s prior approval for outsourcing to an offshore service provider (such as a data center outside Taiwan). |
Are there any restrictions that could hinder the growth and usage of insurtech by insurance companies under data privacy laws?

<table>
<thead>
<tr>
<th>Country</th>
<th>Description</th>
</tr>
</thead>
</table>
| **THAILAND** | Currently, Thailand does not have a consolidated law governing personal data protection. However, if the PDPB is passed under the current format, there are certain restrictions that could hinder the growth and usage of insurtech such as:  
  - an organization (including insurance companies) acting as data controller is required to ensure that personal data in its possession and control is protected from unauthorized access and use, and implement appropriate security measures  
  - cross-border transfer of personal data will also be subject to certain requirements and restrictions  
  - an organization (including insurance companies) acting as data controller should cease to retain personal data as soon as the data owners revoke their consent (unless there is any restriction on revoking consent), after the expiration of the retention period, or personal data that is no longer relevant or in excess of necessity |
| **VIETNAM** | No. Vietnam data privacy regulations remain rather nascent and only impose basic privacy requirements.  
As a general principle, individuals and organizations must grant their prior informed consent to the collection, use and transfer of their personal information. Proper consent requires that the individual or organization collecting, using and/or transferring the personal information, discloses to the person to whom it pertains where the information will be transmitted to and consolidated, how it will be used, to whom the personal information will be transferred and for how long it will be stored.  
An organization should cease to retain personal data as soon as the purpose for which the personal data was collected is no longer being served, or when the agreed-upon retention period expires. |
### AUSTRALIA
- The Privacy Act governs the security obligations relating to personal information.
- Cybercrime Act 2001 criminalizes various computer activities such as hacking, virus propagation, denial of service attacks, and website vandalism.
- Australian Security Intelligence Organisation (ASIO) Act 1979 governs the conduct of Australia's counter-intelligence and security agency and sets out various investigative powers available to ASIO under warrant, including in relation to suspected cybercrime;
- Telecommunications Act 1997 and Telecommunications (Interception & Access) Act 1979 also permits access to communications content held by carriage service providers and licensed telecommunications carriers for law enforcement and national security purposes under warrant.

### CHINA
Yes. Most notably, the following laws contain provisions concerning cybersecurity:
- The National Security Law, which provides the state's focus on safeguarding the security of cyberspace.
- The 9th Amendment to the Criminal Law, which provides that network service providers will be subject to criminal liabilities, if they:
  (i) fail to comply with network security management obligations, causing large-scale dissemination of illegal information or other serious results; or
  (ii) knowingly provide technical support (such as Internet access, server hosting, network storage or communications transmission) to aid crimes committed through information networks.
- The Anti-terrorism Law imposes obligations on telecom business operators and Internet service providers to (i) provide technical support to authorities in connection with investigations for terrorism, (ii) adopt security measures, monitor terrorist content and cooperate with investigations, and (iii) verify customer identity.
- The Draft Cybersecurity Law, which has yet to take effect, will be the first Chinese law that focuses exclusively on cybersecurity and addresses various aspects of cybersecurity in China.

### HONG KONG
The Crimes Ordinance (Cap. 200) criminalizes certain activities, including access to computer with criminal or dishonest intent and destroying or damaging property. Under the Telecommunications Ordinance (Cap. 106), unauthorized access to computer by telecommunications is also an offense. Regulated financial institutions (including insurance companies) may also be expected to have comprehensive risk management systems and policies and disaster recovery plans in relation to cybersecurity risk.

### INDONESIA
No. Indonesia does not have a cybersecurity law, although this is being considered. The government has enacted Presidential Regulation No. 53 of 2017 establishing a national cybersecurity agency. This agency will be a central agency for cyber protection in Indonesia with a focus on national security protection. The regulation is silent on whether this agency can directly assist the private sectors on cybersecurity issues, but the regulation mandates the agency to establish at least technical guides on the identification, detection, protection, monitoring and mitigation of cybersecurity issues. The technical guidelines could be used as guidelines by the private sector, for example, insurance companies.
Are there any laws governing cybersecurity or to mitigate cybersecurity concerns?

<table>
<thead>
<tr>
<th>Country</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan</td>
<td>The Basic Act on Cybersecurity provides the framework of the government’s cybersecurity strategy and basic policies. The Cybersecurity Strategic Headquarters was established under the Cabinet based on this act and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) was established under the Cabinet based on the Order for Organization of the Cabinet Secretariat. The Insurance Supervision Guidelines contain the provisions regarding cybersecurity management as one of the points to be assessed to examine the appropriateness of insurance companies’ system risk management environment.</td>
</tr>
<tr>
<td>Malaysia</td>
<td>The Malaysian Penal Code criminalizes theft, which could extend to conduct involving cybersecurity breaches/theft. The Malaysian Computer Crimes Act 1997 criminalizes unauthorized access to computer material and unauthorized modification of the contents of any computer. In addition, the Malaysian Communications and Multimedia Act 1998 criminalizes unauthorized use of any device and unauthorized interception of any communications and the distribution or advertising of any communications equipment used for interception. The PDPA also has a security principle that requires data users to take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. It should be noted that the SC has issued the Guidelines on Management of Cyber Risks, which apply to capital market entities (but not insurers). Among other requirements, the roles and responsibilities of the board and senior management in the governance of cyber risk is clearly stipulated. The guidelines have also mandated capital market entities to identify a responsible person to be accountable for the effective management of cyber risk. As discussed previously, there is a requirement imposed on insurers to provide the relevant report/notice to BNM in the event of material security breaches and cyber threats. Further, on 9 June 2017, the Deputy Prime Minister of Malaysia announced that the Malaysian government will introduce a new law that is aimed at protecting Malaysians from cybersecurity threats. The Deputy Prime Minister also mentioned that the draft Bill has been handed over to the Attorney-General of Malaysia and will be tabled in the next Parliament sitting, starting 24 July 2017. The National Cyber Security Agency, which was set up in January 2016, will coordinate all efforts in order to ensure that more effective actions may be taken against cybersecurity threats in Malaysia.</td>
</tr>
<tr>
<td>Myanmar</td>
<td>There are no regulations that expressly deal with cybercrime. &quot;Hacking&quot; is considered a criminal offense under the Electronic Transactions Law 2004. There are also suggestions that the government is drafting, or considering, a cybercrime law; however, there have been no publications of a draft version to date.</td>
</tr>
</tbody>
</table>
Are there any laws governing cybersecurity or to mitigate cybersecurity concerns?

<table>
<thead>
<tr>
<th>PHILIPPINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cybercrime Law enumerates and punishes cybercrimes, imposes duties upon service providers, and provides tools for enforcement of cybersecurity.</td>
</tr>
<tr>
<td>Under the Cybercrime Law, a service provider is an entity that provides users of its service with the ability to communicate by means of a computer system. It can also be an entity that processes or stores computer data on behalf of such communication service or users of such service.</td>
</tr>
<tr>
<td>A service provider is expected to do the following:</td>
</tr>
<tr>
<td>• disclose or submit subscriber’s information, traffic data or relevant data in its possession or control to competent authorities within 72 hours after the receipt of an order to submit</td>
</tr>
<tr>
<td>• collect or record by technical or electronic means, and/or cooperate and assist competent authorities in the collection or recording of computer data upon the issuance of a court warrant</td>
</tr>
<tr>
<td>• report to the OCC its compliance with enforcement orders and reporting requirements under the Cybercrime Law</td>
</tr>
<tr>
<td>• immediately and completely destroy computer data subject of a preservation and examination when the required period expires</td>
</tr>
<tr>
<td>• ensure the confidentiality of preservation orders issued</td>
</tr>
<tr>
<td>The Cybercrime Law also enumerates cybercrimes, including computer-related forgery, computer-related fraud and computer-related identity theft. It also punishes certain offenses that violate the confidentiality, integrity and availability of computer data and systems. Among such crimes are illegal access to computer systems, illegal interception of computer data, unauthorized data interference, unauthorized system interference, misuse of devices and cybersquatting.</td>
</tr>
<tr>
<td>Similarly, the DPA also punishes the unauthorized access or intentional breach of any system where personal data is stored.</td>
</tr>
</tbody>
</table>
Are there any laws governing cybersecurity or to mitigate cybersecurity concerns?

**SINGAPORE**

Singapore's Computer Misuse and Cybersecurity Act (Cap. 50A) (CMCA) criminalizes certain activities, including the unauthorized access, use, interception and modification of computers, data and computer services, and empowers the Minister of Home Affairs to act against cybersecurity threats. On 3 April 2017, the Singapore Parliament passed certain amendments to the CMCA to strengthen Singapore's legislative framework for combatting cybercrime. In particular, the amendments seek to extend the reach of the CMCA by criminalizing acts that are enabled by cybersecurity attacks. For example, it would be unlawful for a person to use hacked credit card details, even if the act of hacking was committed by another. In addition, the amendments also targets acts that enable cybercrime, by criminalizing the act of obtaining and the act of dealing in tools that may be used to commit a CMCA offense (for example, hacking tools such as malware).

The Singapore Minister of Communications and Information has also indicated that a new stand-alone Cyber Security Act (CSA) will be introduced in 2017 to strengthen the powers of the Cyber Security Agency to protect Singapore's critical infrastructure and national systems, such as those in the energy and transport sectors, from cyber threats. The proposed CSA is intended to be an omnibus, overseeing cybersecurity of essential services as a whole. Among other things, the proposed CSA will confer power on the Cyber Security Agency's chief as Commissioner of Cybersecurity to investigate threats and incidents to ensure that critical infrastructure and national systems will not be disrupted in the event of a cyberattack. In addition, the proposed CSA also includes proactive and preventive measures that must be undertaken by owners of critical infrastructure, such as conducting regular system audits by a commissioner-approved third party, among others. The Cybersecurity Bill was just released on 10 July 2017 for public consultation.

**TAIWAN**

Taiwan does not have specific or special law governing cybersecurity. However, under the Criminal Code of Taiwan:

- Article 318-1 provides that "a person without reason discloses the secrets of another which he knows or possesses through the use of a computer or other relating equipment shall be sentenced to imprisonment of not more than two years, short-term imprisonment, or a fine not more than five thousand yuan."

- Article 339-3 provides that "a person who for purpose to exercise unlawful control over other's property for himself or for a third person takes property of another by entering false data or wrongful directives into a computer or relating equipment to create the records of acquisition, loss or alteration of property ownership shall be sentenced to imprisonment for not more than seven years; in addition thereto, a fine of not more than seven hundred thousand yuan may be imposed."

- Articles 358 to 363 are offenses against the computer security.

In addition, regulated financial institutions (including insurance companies) are required to have risk management systems and policies and disaster recovery plans in relation to cybersecurity risk.
## Are there any laws governing cybersecurity or to mitigate cybersecurity concerns?

<table>
<thead>
<tr>
<th>Country</th>
<th>Information</th>
</tr>
</thead>
</table>
| **THAILAND** | Thailand has the Computer Crime Act B.E. 2550 (2007) and its recent amendment in 2017 (*Computer Crime Act*) criminalizing certain activities, including the unauthorized access, use and modification of computer data and computer systems. It also empowers the officials under the act to be able to investigate offenses under the Computer Crime Act. These powers include, among others:  
- copying computer data and traffic data of such computer system for which there is reasonable ground to believe that there has been an offense committed, in the case that the computer system is not in the possession of the competent officer  
- accessing a computer system or computer data storage equipment  
- decoding a person’s computer data  
- seizing or attaching a computer system for the purpose of obtaining further details of an offense  
The Thai Cabinet also approved in principle the National Cyber Security Bill in January 2015. It is pending further consideration by relevant authorities before promulgation. The Bill prescribes certain criteria to combat cyberattacks and ensure cybersecurity.  
Please note, however, that there is no specific timeline when the Bill will be passed and it is still subject to changes. |
| **VIETNAM** | On 19 November 2015, Vietnam adopted the Law on Network Information Security, which will take effect on 1 July 2016. This law prescribes, among others, cyber information security activities; civil cryptography products and services; and standards and technical regulations on cyber information security. On 6 June 2017, the government and the Ministry of Public Security (*MPS*) released their first draft of the Law on Cybersecurity (*Draft Law*) for public consultation between 8 June and 8 August 2017. While a definite date is yet to be published, the National Assembly will review and comment on the Draft Law at its fourth meeting later in 2017. |
What innovations are insurance companies and/or regulators looking at implementing?

**AUSTRALIA**

ASIC is considering expanding its regulatory sandbox to potentially allow insurtech start-ups to test a greater number of insurance products without the need to obtain a financial license, subject to certain requirements and limitations.

In the last few years, Australia's largest insurance companies have begun launching venture capital funds and partnering with start-ups to increase the technological sophistication of their products. For example:

- Suncorp Insurance is collaborating with Spanish start-up Traity to create a new micro-insurance offering, which uses blockchain to ensure peer-to-peer transactions made online via a chatbot. The platform, which insures online purchases on websites such as Gumtree and eBay from fraudulent activity, works by using a number of parameters to assess the reputation of both buyer and seller via a virtual agent named Kevin. If reputations are approved, a time stamp is created on blockchain that proves an agreement of transaction from both parties, and in the event of nefarious activity, claimants are insured up to a value of AUD 100.

- Boundless is an artificial intelligence (AI) health companion designed to inspire a healthy lifestyle via its digital messaging, virtual coaching technology, activity challenges and reward partners. The start-up offers partnerships with health and life insurers to help them engage with their customers via the white-label platform, which integrates with over 250 wearables, biosensors and health apps to create a personalized, pro-active coaching tool.

- Insurance Australia Group (IAG) announced that it will launch an insurtech innovation hub in Singapore. The hub, which will be called Firemark Labs, acts as an incubator for IAG to work with start-up, research and technology partners to co-create new products to improve customer experience across Australia, New Zealand and Asia.

- QBE Insurance Group Limited, which is Australia's largest global insurer, is looking to invest up to AUD 50 million in early-stage start-ups and tech ventures to build disruptive solutions in the insurance industry in 2017.

**CHINA**

Fintech/insurtech innovations in China are still a relatively recent phenomenon. As a result, there are no specific insurtech innovations that we are aware of in the insurance sector. As mentioned, the insurance regulator has recently expressed its concern over the lack of regulation and risk control of online insurance businesses conducted by unlicensed online platforms. Accordingly, the insurance regulator has announced that it will clamp down on unlicensed internet insurance businesses as one of its major tasks for 2016.

**HONG KONG**

Hong Kong is still a relatively nascent, emerging fintech/insurtech hub when compared to most established players such as London and New York. However, recent government initiatives and increased marketing are raising awareness. The Hong Kong government launched the Steering Group on Financial Technologies in 2015 to examine the city's potential as a key fintech/insurtech hub, and in the 2016/2017 Budget, the government confirmed it would adopt most of the recommendations made by the Steering Committee in its recent report.

In Hong Kong, some insurers have introduced wearable devices and mobile apps, which are used to track fitness activities of policyholders of life and health insurance products. Using such analytics, the insurers will offer premium discounts to the policyholders based on their level of physical activities, so as to encourage them to exercise regularly. The underwriting risks of such insurers are expected to improve as a result.
What innovations are insurance companies and/or regulators looking at implementing?

**INDONESIA**
We are aware some insurance companies are selling online insurance products. However, the practices are only related to simple insurance products such as travel insurance protection with minor sum-insured values. In addition, most insurance companies are providing online accounts but more for the purpose of allowing customers to check their claims and their investment funds (for unit-linked products). This is primarily as regulation is still old school and requires, for example, that hard copies of insurance policies are provided to customers.

**JAPAN**
In Japan, as mentioned in question 3 above, the direction and contents of insurtech innovations to be implemented are still under study and discussion by the regulator and market players, including insurance companies.

Since 2015, some non-life insurance companies introduced new insurance products utilizing telematics. In spring of 2016, it was reported that many leading life and non-life insurance companies would strengthen R&D on products utilizing insurtech such as non-life insurance products using Internet of Things information and life insurance products using genetic information. In spring of 2017, it was also reported that large insurance companies are developing fintech insurance products utilizing AI and big data.

**MALAYSIA**
As mentioned in question 3 above, BNM has launched the Financial Technology Regulatory Sandbox Framework. In addition, BNM indicated that it intends to regulate the establishment and operations of the product aggregators by publishing requirements on the same in 2016. However, this has been delayed to 2017/2018 to enable BNM to draw on the experience from the regulatory sandbox.

Further, BNM, through FTEG has rolled out an initiative called "Fintech Hacks," which allows the public to submit their innovative ideas through, among others, its website on the improvements to the financial services sector by harnessing innovation and technology.

To date, banks in Malaysia have publicly announced the implementation of innovation and accelerator programs (rather than insurance companies). We expect insurance companies to undertake similar initiatives in the near future (as there have only been a handful that have indicated or collaborated in the launch of accelerator programs).

**MYANMAR**
No deviation is currently permitted from the set insurance products. We consider that significant innovation will occur once the new insurance laws are released.

**PHILIPPINES**
Sun Life of Canada (Philippines), Inc., a life insurance provider in the Philippines, and Voyager Innovations, a digital innovations arm of a major telecommunications company, have recently entered into a strategic partnership for the development of insurtech services for emerging markets. One of these initiatives is to implement the country's first insurance and micro savings program for public school students. The initiative is supported by the BSP and the IC.
### Market Trends

**Singapore**

In April 2015, the MAS launched a web aggregator called compareFIRST, which allows consumers to compare the premiums and features of life insurance products and acts as a direct purchase channel, allowing people to buy simple life insurance products without commissions and financial advice. Since then, many banks and insurance companies have announced innovation hubs or accelerator programs, with the support of the MAS and other relevant government bodies, including the IDA (now merged with the MDA to constitute the IMDA).

In late 2016, MAS launched its fintech regulatory sandbox experiment in order to encourage more fintech experimentation so that promising innovations can be tested in the market and have a chance for wider adoption. As of June 2017, only one sandbox experiment has been accepted by the MAS and publicly announced. The sandbox is an area of active innovation and there are market trends suggesting continued application of the sandbox to insurtech developments in Singapore.

**Taiwan**

In October 2015, the FSC allowed insurance companies, within certain limits, to invest in business-related or auxiliary to financial technology-related business (such as big data analysis, software design and Internet of Things).

**Thailand**

We have seen certain insurance companies/brokers using fintech/insurtech innovations as new channels for offering new insurance products to customers. Certain insurance companies have partnered with these fintech/insurtech operators, such as AgentMate, Savinsure, Directasia.com, etc., in offering their insurance products through this channel.

From the regulator’s perspective, the OIC has launched the utilization of a regulatory sandbox in Thailand in July 2017 to enable insurers, agents, fintech/insurtech players to test their innovations. This regulatory sandbox is still at an initial stage and it remains to be seen whether it would attract intention of fintech/insurtech developers. In addition, the OIC has also announced the new notifications on enterprise risk management, which aim to improve the standard of internal control within insurance companies in Thailand; this would be in line with the rapid changes in the insurance business sectors given the forthcoming innovations and the fierce competition among existing and new players in the market.

From the insurers’ perspectives, we have seen many players’ movements in relation to introducing new innovations to the market, particularly on motor and health insurance. Insurance products have been developed to fit into the customers’ daily life; for example, motor insurance products in which the coverage can be activated and deactivated at the customer’s sole intention, or health insurance products, which factor in technology to facilitate and monitor the customer’s behavior on a daily basis. More innovations are expected to be introduced, especially with the recent introduction of the regulatory sandbox regime.

**Vietnam**

Fintech/insurtech is new in Vietnam, but we have seen certain insurance companies starting to look for fintech/insurtech innovations in analyzing big data, which can help them to determine their target customers and business decisions.
## Have there been fintech/insurtech-related cases (including competition and/or data privacy) in Asia Pacific?

<table>
<thead>
<tr>
<th>Country</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AUSTRALIA</strong></td>
<td>There have been no specific cases in relation to fintech/insurtech cases to date.</td>
</tr>
<tr>
<td><strong>CHINA</strong></td>
<td>There have been quite a number of cases where the operation of P2P lending platforms has been characterized as criminal offenses involving illegal fundraising or unlicensed deposit taking, and the persons found to be responsible for these platforms have been subject to criminal sanction.</td>
</tr>
<tr>
<td><strong>HONG KONG</strong></td>
<td>There are no specific cases by the financial regulators so far.</td>
</tr>
<tr>
<td><strong>INDONESIA</strong></td>
<td>We are not aware of any fintech/insurtech cases (noting that there are no law reports in Indonesia).</td>
</tr>
<tr>
<td><strong>JAPAN</strong></td>
<td>There have been a number of cases where administrative sanctions were imposed on financial institutions due to the lack of appropriate management of customer information; however, such cases were mere loss, leakage or misuse of customer information and were not necessarily fintech/insurtech-related cases. We are not aware of any fintech/insurtech-related competition cases.</td>
</tr>
<tr>
<td><strong>MALAYSIA</strong></td>
<td>There are no specific cases by the financial regulators so far.</td>
</tr>
<tr>
<td><strong>MYANMAR</strong></td>
<td>There are no specific cases by the financial regulators so far.</td>
</tr>
<tr>
<td><strong>PHILIPPINES</strong></td>
<td>In a case decided by the NPC on 28 December 2016, the National Privacy Commission (NPC) recommended the criminal prosecution of the Chairman of the Philippine Commission on Elections (Comelec) for his “gross negligence,” which resulted in the massive leak of voters’ registration information involving around 77 million voters. In so ruling, the NPC noted that the Comelec’s platforms, although secured with specific measures, were designed without clear lines of responsibility, continuous testing and feedback mechanisms, and contingency and response plans in case of breach. The NPC also highlighted the Comelec chairman lacked appreciation of the fact that “data protection is more than just implementation of security measures, but must begin from the time of collection of personal data, to its subsequent use and processing, up to its storage or destruction.” The NPC found that the chairman failed to promulgate a data privacy and protection framework, which ultimately led to the data leak. The hackers directly responsible for the data leak are also currently being prosecuted.</td>
</tr>
</tbody>
</table>
### SINGAPORE
On 17 March 2016, the Competition Commission of Singapore issued an infringement decision against ten financial advisers in Singapore for engaging in an anticompetitive agreement to pressure their competitor, iFAST Financial Pte. Ltd., to withdraw its offer of a 50% commission rebate on competing life insurance products on the Fundsupermart.com website. The ten financial advisers were fined between SGD 5,000 and SGD 405,114, depending on each financial advisor's respective life insurance business turnover and aggravating and mitigating factors. This is the first case involving market access and restriction of market access involving firms in the financial services industry and highlights that the Competition Commission of Singapore will enforce the law where necessary to ensure that new and innovative players can access the market and compete fairly in Singapore.

### TAIWAN
With regard to P2P lending, the FSC issued a news release on 28 April 2016 questioning the following:

- guarantee of fixed return and taking funds from the lender before a loan agreement is signed may constitute deposit taking regulated under the Banking Act
- investment return shall not exceed 20% per annum (the maximum annual interest rate permitted under the Civil Code)
- high return with low cost and low risk could constitute fraudulent advertisement regulated by the Fair Trade Act
- membership with high return may constitute multilevel marketing regulated by the Fair Trade Act

### THAILAND
There are no specific cases by the financial regulators so far.

### VIETNAM
There are no specific cases by the financial regulators so far.
### WHAT ARE THE MOST IMMEDIATE CHALLENGES TO INSURTECH INNOVATION?

#### AUSTRALIA
- The high costs of development and innovation – While there is high demand from insurers looking for new technologies to improve customer service and transform operational models, there are still many insurance companies that do not have a budget allocated for innovation, or someone actually responsible for innovation. See KPMG’s insurtech research at: [https://home.kpmg.com/au/en/home/insights/2017/03/insurtech-dilemma-insurance-technology.html](https://home.kpmg.com/au/en/home/insights/2017/03/insurtech-dilemma-insurance-technology.html).
- Regulation – High levels of regulation from ASIC and APRA present a significant barrier to entry. Industry groups are seeking support form the Australian government for increased flexibility to support emerging micro-insurance and quasi-insurance models (for example, self-funded excess and peer-to-peer insurance), which are not readily facilitated by current models. See [https://fintech.treasury.gov.au/australias-fintech-priorities/](https://fintech.treasury.gov.au/australias-fintech-priorities/)

#### CHINA
- Lack of centrally coordinated regulator for fintech/insurtech business – While there are various regulators overseeing specific financial service sectors, they have not put in place a coordinated scheme to address their overlapping jurisdiction, which often results in a lack of specific guidance and supervision of fintech/insurtech innovation.
- Difficulty in securing licenses – Due to the lack of specific rules and regulations, it has been difficult to obtain the appropriate licenses required for conducting fintech activities, which constantly result in the legality of the relevant fintech business being questioned or challenged.
- Cybersecurity issues

#### HONG KONG
- Complexity of the sector-specific regulatory regime in Hong Kong and the different types of licenses and/or authorization needed
- The high costs of development and innovation
- Cybersecurity – As the sophistication of cyber criminals have evolved, it is crucial to ensure that there are robust policies and systems in place to address cybersecurity. Failure to do so may also affect customer confidence.

#### INDONESIA
- Regulations – The government acknowledges that it is likely to be behind market developments in regulating fintech/insurtech activities. Consequently there is less clarity for businesses as to how matters may be regulated, and reliance on older regulations, which may not be as conducive to the fintech/insurtech sector (for example, written consent for data use and transfer). In November 2016, Bank Indonesia established a dedicated fintech office within its organization to assist fintech start-ups in risk assessment, licensing coordination and a regulatory sandbox. The effectiveness of this fintech office remains to be seen.
- Technology – Local technology may not be sufficient to accommodate the development of fintech products.
- Customers – Although internet utilization is becoming more common in Indonesia and Indonesians are more tech-savvy than before, customers may take time to accept fintech/insurtech. Currently most selling of financial products is personal in nature (for example, telemarketing and agents). Customers will need more assurance and more time to accept fintech/insurtech services.
What are the most immediate challenges to insurtech innovation?

<table>
<thead>
<tr>
<th>Country</th>
<th>Challenges</th>
</tr>
</thead>
</table>
| JAPAN   | - The lack of appropriate legislation covering the cross-sectoral and cross-border development of fintech/insurtech  
- The high costs of development and innovation  
- The lack of skilled personnel who have the capacity in both financial and technological areas and the limited mobility of such skilled personnel |
| MALAYSIA| - Regulatory and compliance – Currently, many fintech/insurtech businesses do not fall squarely within any particular regulatory regime in Malaysia. Until such time as there are clear regulatory prescription governing fintech/insurtech companies and their businesses, fintech/insurtech companies must evaluate their fintech/insurtech innovation at the outset and question whether their business activity can be undertaken without the fintech/insurtech company becoming a regulated entity, or whether it would have to seek appropriate licenses or approval and incorporate internal compliance frameworks such as anti-money laundering procedures. An understanding of the consumer protection and liability exposures may also be lacking.  
- The high costs of development and innovation – Particularly for start-ups, the lack of funding has not been adequately dealt with and hinders access to facilities, especially for the fintech sector.  
- Skill and talent – The necessary infrastructure, talent and skill set to catalyze fintech/insurtech developments in Malaysia are lacking. Guidance will have to be sought from more developed markets. |
| MYANMAR | - Existing restrictive regulations  
- Extent of insurance penetration and understanding within Myanmar  
- Limited scope of electronic banking among the population – It is estimated that a significant number of Myanmar citizens (well over 50%) do not have bank accounts. While mobile wallets and other payment mechanisms are becoming more popular, this will need to expand before uptake of insurtech can be linked to fintech innovations as well. |
### MARKET TRENDS

**PHILIPPINES**
- Absence of regulations – Because of the absence of, or gaps in the, regulations on fintech/insurtech, there is uncertainty on whether a proposed new product or service would receive regulatory approval. In such cases, the fintech/insurtech provider has the burden of convincing the regulator that the product or service does not fall under any legal prohibition and would bring benefit to the economy/consumers.
- Cybersecurity – Local networks, including government networks, and websites remain vulnerable to hacking.
- Unregulated digital money such as Bitcoins can be used as a medium for illegal transactions, and can also expose consumers to risk.
- Accessibility for potential consumers – Around 40% of the municipalities in the country do not have any banking presence, and many cannot access app-based financial services in far-flung areas.

**SINGAPORE**
- The high costs of development and innovation; for start-ups, the lack of finances
- Regulatory and compliance – Fintech/insurtech businesses may not always fall squarely within any particular regulatory regime in Singapore, and in certain instances, such as the use of virtual currencies and blockchain technology, there is ongoing uncertainty over the approach to regulation. The regulatory sandbox approach seeks to mitigate the uncertainty over the application of laws and regulations to new fintech/insurtech businesses, and fintech/insurtech are encouraged to make use of such regulatory framework to continue innovation in their spheres notwithstanding such uncertainty.
- Cybersecurity – As the sophistication of cybercriminals has evolved, it is crucial to ensure that there are robust policies and systems in place to address cybersecurity. Failure to do so may also affect customer confidence.
- The lack of skilled employees that are able to effectively develop, utilize and apply fintech/insurtech innovations
- Data protection privacy – Many insurtech companies are making use of big data capabilities and analytics. Any misuse or leakage of such analytics might be in breach of data protection laws and pose a reputational risk for insurers.

**TAIWAN**
- Heavy regulations and high capital requirements for start-ups to obtain the relevant licenses impose a high cost on development and innovation
- No special cybersecurity laws or regulations (only general criminal liabilities under the Criminal Code)
- Lack of patent and know-how to develop fintech
What are the most immediate challenges to insurtech innovation?

<table>
<thead>
<tr>
<th>Country</th>
<th>Challenges</th>
</tr>
</thead>
</table>
| Thailand | • Lack of supporting legislation and regulations for governing the secure implementation of fintech/insurtech innovation, including consolidated data privacy protection laws. Current regulations are still unsupportive for small players in the market.  
• Thai consumers still do not have much knowledge about fintech/insurtech innovations and still prefer traditional methods when transacting.  
• Small user base and lack of funding and finances for fintech/insurtech innovation.  
• Regulatory and compliance – Insurtech businesses may not always fall squarely within any particular regulatory regime in Thailand. The regulatory sandbox approach seeks to mitigate the uncertainty over the application of laws and regulations to new insurtech businesses.  
• There is no proper ecosystem to support the development and improvement of insurtech innovations. The regulators are aiming to address this matter, but it would generally take time and support from many parties.  
• General public has very limited knowledge and understanding on insurance business. For example, young generation of innovation developers find it has nowhere to design and fit their innovations to the insurance sector. This limits initiatives on insurtech innovations. In order to encourage insurtech innovation, a basic understanding of insurance business must be portrayed to the developers.  
• The Thai insurance industry comprises several big players dominating the market. These insurers have a more profound understanding of the business and are extremely active in spotting opportunities to develop insurtech innovations. This makes it difficult for new insurtech start-up to make a breakthrough entry to the market. Even though they were able to do so, there is a possibility that they would need to partner with the insurer or eventually sell the business. |
| Vietnam | • The majority of consumers in Vietnam are generally still unfamiliar with fintech/insurtech innovations. As such, consumers prefer the traditional means of financial instruments, which seem to be safer and easier to use.  
• Vietnam lacks skilled and trained employees specializing in fintech/insurtech innovations.  
• Despite regular legislative updates, the legal framework of Vietnam has not effectively caught up with the rapid development of technology in general and fintech/insurtech in particular. |
### Market Trends

The publication reflects the position as of November 2017. Specific advice should be obtained in this evolving and complex area.

**Australia**: Fintech/insurtech has been, and will continue to be, a key enabler in designing better and more efficient work processes and creating new business models that will deliver higher growth, cost savings and better services for industry participants.

**China**: Fintech/insurtech will likely continue to play an important role in the financial services industry in China given the policy objective of the Chinese government to promote fintech/insurtech as well as the increasing use of digital devices by Chinese consumers.

The Chinese government is considering setting up a centralized financial and monetary regulator that may have comprehensive power to regulate most (if not all) fintech/insurtech activities. This has been considered one of the most significant impacts of fintech/insurtech innovation on the regulation of the financial services industry in China.

**Hong Kong**: Fintech/insurtech will likely be a key enabler in designing better and more efficient work processes and creating new business models that will deliver higher growth, cost savings and better services for industry participants.

**Indonesia**: The impact on financial services is just occurring (for example, mobile banking). There is a huge potential for online financial services in Indonesia, and with the appropriate products, education, security and regulation, fintech/insurtech will, no doubt, grow. Innovation developed offshore is likely to come onshore.

**Japan**: Fintech/insurtech is expected to be a key driver in introducing new business opportunities and business models in the financial sector. It will also likely promote competition between existing financial institutions and new market entrants.

**Malaysia**: The most imminent impact of fintech/insurtech on the financial services industry in Malaysia will likely be in the banking and insurance (please refer to question 15 below) sectors.

In respect of the banking sector in particular, there has been an evolution in payment methods. Further, CIMB and Maybank (which are among the largest banking institutions in Malaysia) have also implemented innovation and accelerator programs in Malaysia.

Also, the regulation of crowdfunding platforms and peer-to-peer lending operators by the SC encourages alternative lending platforms, which provide an online marketplace for lenders to exercise greater discretion and choice, based on their risk appetite. There will also be lower costs of borrowing and greater transparency in the communications chain between borrowers and lenders.

Finally, we foresee that the use of technology will eventually displace traditional labor-intensive working models and result in greater automation in respect of client-fronting activities and decision-making processes, through the use of robo advisers, artificial intelligence and blockchain technology, reducing reliance on skill-based labor.
## MARKET TRENDS

The publication reflects the position as of November 2017. Specific advice should be obtained in this evolving and complex area.

### MYANMAR

The Myanmar population is fast developing a mobile and online presence, meaning that technological development and innovation is welcome in the country. As such, with relaxation of the insurance laws permitting scope for growth and innovation in the insurance industry, it is highly likely that insurtech innovation will become widely utilized within Myanmar.

### PHILIPPINES

Fintech/insurtech will be critical in ensuring that financial services are readily available for those that currently cannot access them. According to the BSP, around 70% of the working adults today are “underbanked” or “unbanked.”

In addition, the rise in fintech/insurtech has already led to more cooperation between banks and fintech entities. Banks have also explored options that allow for a digital transition in its operations.

However, local networks, including government networks, and websites remain vulnerable to hacking, while unregulated digital money such as Bitcoins can be used as a medium for illegal transactions.

### SINGAPORE

Fintech/insurtech will likely be a key enabler in designing better and more efficient work processes and creating new business models that will deliver higher growth, cost savings and better services for industry participants.

### TAIWAN

Traditional financial products or services may be replaced by new products or services provided by start-ups or multinational high-tech or companies.

### THAILAND

The development of fintech/insurtech technologies and innovations will continue to shape customer behavior, business models, and the structure of the financial services industry, and will become new trends that should be closely monitored. It would also urge big players in the marker to be more innovative and promote competition among all of them. From the regulators standpoint, the regulators are forced to have a better understanding of new innovations and business trends in order to catch up with the rapid changes in the business sector, so that appropriate rules and regulations can be issued and implemented in such a way that would not only help regulate new innovations, but also support the implementation that would, in turn, provide benefit to the general public as a whole. From the customers’ standpoint, fintech/insurtech innovations could redefine the way in which financial services industry are conducted and it could reinvent. Traditional method of communication between the customers and business operators are likely to be reinvented. Most importantly, insurtech innovation would also serve as a key function to reconnect the customers and the business operators. The development of fintech/insurtech would also offer more business opportunities to both young generation of developers and players within the financial service industry. It is also likely to promote cooperation within the industry, for example, joint venture. Existing players could become key investors in new fintech/insurtech start-ups. There will also be more opportunities for M&A activities in a later stage as it serves as a way to either expand or protect the ongoing business.

### VIETNAM

The development of fintech/insurtech innovations is expected to introduce new business opportunities and business models in the insurance, banking and financial sectors. These are expected to deliver higher growth and efficiency and better services.
## What insurtech trends or disruptions may impact insurance companies?

<table>
<thead>
<tr>
<th>Country</th>
<th>Trends/Disruptions</th>
</tr>
</thead>
</table>
| **AUSTRALIA** | We can expect to see a rise in insurance companies acquiring or teaming up with tech-focused companies (including digital insurance start-ups or telematics-related companies) in order to deliver new products and better price risk. The three main trends or disruptions include:  
  - Increase in collaboration between start-ups and incumbents: high barriers to entry to the insurance industry could restrict a wave of new stand-alone e-insurance brokers, which would need to work with traditional insurance companies.  
  - Insurance telematics: with insurance telematics, insurers can have better information and can expect a rise in usage-based insurance and dynamically adjusted premiums, moving away from conventional static premiums. Further, insurance telematics can help improve risk management, drive cost down for claims process, enhance customer loyalty through creating opportunities for regular contact and potentially open up new possibilities for sales channels and revenue-generating services in partnership with businesses from other sectors.  
  - Improved data analytics: With improved data analytics, the old-fashioned actuarial tables of insurance companies can be enhanced with real-time data and dynamic pricing. Wearable tech and telematics also give companies more personalized data. |
| **CHINA** | It remains to be seen if internet insurance will continue to grow in China in the future, given the previous regulatory action taken by the Chinese insurance regulator. |
| **HONG KONG** | We expect to see insurance companies seek to acquire or team up with non-insurance tech players such as new digital insurance start-ups or telematics-related companies in order to deliver new offerings and better price risk, extend the value chain and have greater overall efficiency. With big data, we also expect to see more insurers better adopt end-to-end analytics solutions that cross the entire insurance value chain. In doing so, they hope to gain an enriched, single client view and the ability to execute a targeted pipeline.  
  
  Another area may be "just-in-time" insurance. It has also been suggested that the traditional concept of insuring an asset over many periods is outdated, and that instead, the business should move to a more transactional consumption model where just-in-time insurance is delivered on mobile and underwritten in seconds.  
  
  Use of telematics, which is becoming more prevalent for insurers in Hong Kong, will enable insurers to accumulate customers' voluminous behavioral information. This will allow insurers to have a deeper insight of their customers, which in turn will assist them in formulating new directions for products and pricing their risks more accurately. Insurers will need to be mindful of the need to ensure the accuracy and reliability of these information. Insurers will also need to devise controls and systems for these analytics to be appropriately integrated into the offering to the customers (for example, offering premium discount, determining future premiums, etc.). As the use of such analytics may directly affect the customers, any incidents of misuse, leakage or improper application of such analytics will pose a reputation risk for the insurer. |
### Indonesia

In practice, distribution of products is personal in nature (for example, telemarketing and agents). If the regulations are not sufficient to give customers protection, the customers may stay with conventional products and distribution channels. The key issues are to ensure courts will accept digital evidence more readily and that regulation is updated so that e-policies can be issued and digitalization embraced. Innovation developed offshore is likely to come onshore. To the extent that customers embrace digitalization, this will allow small or start-up insurance companies to leapfrog and become major insurers without the existing expense incurred with using telemarketing and agents.

Insurance companies will seek to acquire or team up with non-insurance tech players such as new digital insurance start-ups or telematics-related companies in order to deliver new offerings, better price risk, extend the value chain and have greater overall efficiency. As a further example, insurance companies are also looking to mine data sets to identify underwriting opportunities for those who suffer chronic illnesses such as dementia and obesity. With big data, we also expect to see more insurers better adopt end-to-end analytics solutions that cross the entire insurance value chain. In doing so, they hope to gain an enriched, single client view and the ability to execute a targeted pipeline.

### Japan

As mentioned in question 3 above, the next trends are still under study and discussion by the regulator and market players, although we already see some initial moves such as the formation of a JV by a car manufacturer and a non-life insurer on telematics insurance development. In the discussions held in the study group, it was pointed out that new market entrants from different business areas and the commoditization of risks due to technical innovation in various areas would disrupt traditional business model of insurance companies. Although it is not currently easy to expect the extent and speed of disruption, there will be an existing trend of insurance companies making significant investments in R&D on products utilizing insurtech. Please also see question 11 above.

### Malaysia

Insurance companies will be disrupted at key pressures across the value chain.

In respect of product distribution, online aggregators that assist customers with comparisons of insurance coverage may displace traditional distribution channels, which are primarily manpower-focused (that is, through insurance agents and distributors). With such information easily accessible through a “one-click solution,” there will be greater competition between insurers to leverage on technology to modify their traditional processes and allow for a shorter time for the issuance of insurance policies while at the same time ensuring compliance with underwriting risks measures.

Self-driving and pay-as-you-go rentals may affect traditional insurance underwriting models development based on a single or paper ownership structure. Risk determination for underwriting models may also shift toward the use of personalized statistical data through telematics.

We expect insurance companies to vary their business models in the future, whereby they may choose to partner with or acquire non-insurance technology players to incorporate business models that are more data intensive (and less manpower and capital intensive) and platform/infrastructure based. This could result in greater access to more innovative product offerings, with better value for end customers. The greater utility value derived from the use of big data by insurers will also assist with ensuring such outcomes.
### What insurtech trends or disruptions may impact insurance companies?

<table>
<thead>
<tr>
<th>Country</th>
<th>Trend or Disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MYANMAR</strong></td>
<td>The relaxation of market regulation and the opening the market to foreign insurance companies will be a significant development within the next year.</td>
</tr>
<tr>
<td><strong>PHILIPPINES</strong></td>
<td>We expect insurance companies partnering with insurtech and technology entities to help them develop their technology and business strategies.</td>
</tr>
<tr>
<td><strong>SINGAPORE</strong></td>
<td>Insurance companies will seek to acquire or team up with non-insurance tech players such as new digital insurance start-ups or telematics-related companies in order to deliver new offerings, better price risk, extend the value chain and have greater overall efficiency. As a further example, insurance companies are also looking to mine data sets to identify underwriting opportunities for those who suffer chronic illnesses such as dementia and obesity. With big data, we also expect to see more insurers better adopt end-to-end analytics solutions that cross the entire insurance value chain. In doing so, they hope to gain an enriched, single client view and the ability to execute a targeted pipeline. Another area may be “just-in-time” insurance. It has also been suggested that the traditional concept of insuring an asset over many periods is outdated, and that instead, the business should move to a more transactional consumption model where just-in-time insurance is delivered on mobile and underwritten in seconds. We may increase accessibility to insurance in Singapore. The MAS’ compareFIRST web aggregator was successful with more than 180,000 visits within the first three months of its launch and we may see the cost of insurance become lower, providing access to lower-income consumers. In addition, the insurance sector has seen new contenders come up with the aim of addressing the shortcomings in user experience and analytics of compareFIRST. This ensures a more efficient &quot;aggregator&quot; experience where customers have a smoother experience comparing the latest offerings. Hence, we may see the cost of insurance become lower, providing access to lower-income consumers. We expect to see enhanced customer service in insurtech. For example, some insurance companies have launched a self-learning virtual assistant, which is meant to provide instant answers to operational inquiries, and thus enabling frontline staff to focus on dealing with more complex queries. Other insurtech apps are working on improving the notification system for payment of premiums and renewals. In doing so, insurance companies can heighten efficiency in serving customers, which might help expand the insurance company’s customer base. We can also expect a rise in usage-based insurance and dynamically adjusted premiums. Companies may begin to offer insurance schemes based on lifestyles instead of traditional factors such as age and location.</td>
</tr>
<tr>
<td><strong>TAIWAN</strong></td>
<td>Taiwan insurance companies are discussing how to use big data to conduct risk analysis and offer new products to customers. They are also considering downsizing their sales force and selling products through banks and digital channels. The existing sales channels of insurance (such as insurance solicitors, brokers and agents) may be reduced. From KYC (Know Your Customer) to KYDC (Know Your Digital Customer), Taiwan insurers need to develop new technology to know digital customers.</td>
</tr>
</tbody>
</table>
What insurtech trends or disruptions may impact insurance companies?

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| THAILAND  | We expect to see insurance companies more involved in insurtech innovation in many areas, whether by themselves or through partnership with other insurtech operators, in order to create efficiency in providing insurance services to customers.  
Potential areas that insurtech innovation could play roles in insurance business might include the offering of insurance products, price comparison between insurance products and policy underwriting, claims management services.  
We can also expect to see competition between insurance companies to capture this new business opportunity. Insurance companies are likely to be forced to improved its products to catch up with the customers’ lifestyle and for this, a close monitoring and research of the customer’s interest and behavior would be the key focus. They may also look to invest in venture capital companies focusing on insurtech start-ups and must also look for recruitments of young generation with potential to drive the organization toward the current trends. |
| VIETNAM   | We expect to see insurance companies more involved in insurtech innovation in many areas. Development of insurtech will offer more financial choice to customers, which will have significant impact on the market of insurance business. We expect to see more and more insurance companies cooperate with insurtech players to diversify their insurance products, diversify their distribution channels and facilitate the development of the insurance market in Vietnam. In particular, electronic transactions will be developed to supersede traditional transactions. In doing so, insurers will improve their competitive advantage and bring more benefit to the insurance purchasers as well. |
For more information about this guide, please contact:

**AUSTRALIA**

Adrian Lawrence  
Principal  
Tel: +61 2 8922 5204  
adrian.lawrence @bakermckenzie.com

**CHINA/HONG KONG**

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

**INDONESIA**

Mark Innis  
Foreign Legal Consultant  
Tel: +62 21 2960 8618  
mark.innis @bakernet.com

**JAPAN**

Jiro Toyokawa  
Partner  
Tel: +81 3 6271 9457  
jiro.toyokawa @bakermckenzie.com

**MYANMAR**

Jo Daniels  
Principal  
Tel: +95 1 9255095 ext. 8857  
jo.daniels @bakermckenzie.com

**PHILIPPINES**

Elizabeth Opena  
Partner  
Tel: +63 2 819 4941  
elizabeth.opena @quisumbingtorres.com

**MALAYSIA**

Brian Chia  
Partner  
Tel: +60 3 2298 7999  
brian.chia @wongpartners.com

**SINGAPORE**

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

**THAILAND**

Sorachon Boonsong  
Partner  
Tel: +66 2636 2000 ext. 4038  
sorachon.boonsong @bakermckenzie.com

**TAIWAN**

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

**VIETNAM**

Chi Lieu Dang  
Partner  
Tel: + 84 4 3936 9341  
chilieu.dang @bakermckenzie.com
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