Baker McKenzie.

Asia Pacific Guide to Insurtech Innovation and Utilization

TRANSACTIONAL POWERHOUSE

Leading and closing complex deals – every day

Contents

01 Executive Summary

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 be too early to herald insurtech's success, one thing is for certain: insurtech is here to stay.

In the same vein, the regulatory regimes across multiple jurisdictions have had to evolve 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 10 jurisdictions, in respect of concerns that may arise in the development and utilization of insurtech.

Regulatory Environment for Innovation

01 Regulatory Environment for Innovation

Who are the relevant regulators in the region?

CHINA	In China, the regulators of Insurtech are as follows:: ▪ China Banking and Insurance Regulatory Commission ("**CBIRC**"): the CBIRC is responsible for the overall supervision and administration of banking and insurance industries, participates in the drafting of important laws and regulations on banking and insurance and formulates rules and measures for prudential supervision and conduct regulation of banking and insurance. ▪ Financial Stability and Development Commission of the State Council: as the deliberation and coordination body of the State Council for major issues concerning financial stability and reform and development, the Financial Stability and Development Commission reviews major plans for reform and development of financial industries, provides overall instructions on the reform, development and regulation of financial industries, and coordinates major issues in financial regulation. ▪ The People's Bank of China: the People's Bank of China takes the lead in establishing the framework of macro-prudential administration, drafts major laws and regulations in the financial sector and other relevant laws and regulations, and formulates the basic institutions for prudential supervision. The People's Bank of China also drafts plans for the reform, opening up and development of financial industries, conducts comprehensive research on and coordinates major issues in financial industries, and promotes the balanced and healthy development of financial industries. Since 2019, the People's Bank of China has issued the Fintech Development Plan (2019-2021) and the Fintech Development Plan (2022-2025). In addition to the aforesaid entities, there are several entities that may involve in the regulation of insurtech. In respect of cybersecurity issues, the Ministry of Public Security will regulate compliance with relevant laws and regulations in the provision of fintech/insurtech together with the Ministry of Industry and Information Technology. The Cyberspace Administration of China will jointly regulate internet information service with the Ministry of Industry and Information Technology, especially on blockchain-based information services.
HONG KONG	The Insurance Authority (**IA**) is Hong Kong's insurance regulator overseeing the financial conditions and operations of authorized insurers and insurance intermediaries. 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**) regulates 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.

01 Regulatory Environment for Innovation

Who are the relevant regulators in the region? (cont'd)

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. 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. See Question 2.
MALAYSIA	Several regulators oversee the financial services sector, and each such regulator would have oversight of their respective regulated institution. Specifically: ▪ 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. ▪ Securities Commission Malaysia (**SC**) would regulate fintech/insurtech activities affecting the capital markets and participants. Given that fintech/insurtech involves technology and data, it is also likely to fall within the purview of the following: ▪ 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"

01 Regulatory Environment for Innovation

Who are the relevant regulators in the region? (cont'd)

PHILIPPINES	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.
SINGAPORE	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 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.
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). In August 2020, the FSC published the Fintech Development Roadmap, which includes the FSC's vision, principles and eight dimensions of fintech development in Taiwan from 2021 to 2023.

01 Regulatory Environment for Innovation

Who are the relevant regulators in the region? (cont'd)

THAILAND	The main regulator is the Office of Insurance Commission in charge of insurance companies operating in Thailand. The office recently established the Center of InsurTech to support and promote insurtech innovation. Depending on the specific activities, other regulators may be involved, including the following: ▪ Ministry of Finance – oversees financing, securities and credit financier businesses and financial institutions. ▪ Bank of Thailand – oversees commercial banks, payment service providers, financing businesses, and other financial institutions, which range across money lending, currency exchange, etc. ▪ Securities and Exchange Commission – the regulator in charge of securities business and digital asset business, including public fundraising through capital markets. ▪ Ministry of Commerce – oversees business operations of a company incorporated in Thailand, whether private, public or listed. ▪ Electronic Transaction Commission under the Prime Minister – oversees electronic transactions regulated under the Electronic Transaction Act. ▪ The Ministry of Digital Economy and Society – regulating online content, computer data retention and computer crimes.
VIETNAM	No single authority 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 Public Security (**MPS**) is responsible for cybersecurity. ▪ 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.

02 Regulatory Environment for Innovation

What is the attitude and what are the policy views of the regulator in relation to insurtech (if any)?

CHINA	According to the Fintech Development Plan (2022-2025), the general attitude of Chinese regulators towards fintech is to encourage the development of fintech to provide “digital, intelligent, green and equal” financial services while enhancing prudential supervision on fintech. In the Guiding Opinions on Promoting the High-quality Development of Banking and Insurance Industries (No. 52 [2019] of the China Banking and Insurance Regulatory Commission), the CBIRC emphasized that financial innovation requires strong technological support and insurance institutions should fully utilize new technologies, such as artificial intelligence, big data, block chains and biometrics, to improve service quality, to lower service costs and to strengthen business management. Art. 50, para. 2 of the Measures for Regulation of the Internet Insurance Business (Order No. 13 [2020] of the China Banking and Insurance Regulatory Commission) provides that insurance companies should promote the application of new technologies to insurance business to improve their operation efficiency and consumers’ experience. On the other hand, the Measures for Regulation of the Internet Insurance Business emphasizes on risk control and consumer protection, in order to achieve orderly and healthy development of insurtech.
HONG KONG	Hong Kong regulators have reacted positively and encourage fintech/insurtech innovation in the following ways: ■ Funding – The Hong Kong government has been providing funding to the Fintech Proof-of-Concept Subsidy Scheme, which aims to encourage financial institutions such as banks, insurance companies, securities firms and asset management companies to partner with fintech companies to conduct proof-of-concept projects on innovative financial service products. Further, the Hong Kong government has been providing funding and/or subsidies for eligible companies to hire fintech talents and for practitioners in the insurance and securities sectors to attend fintech trainings. ■ Support – The IA, HKMA and SFC have launched various initiatives to promote insurtech development in Hong Kong. These include, for example: - **Insurtech/Fintech Sandbox** – The IA, HKMA and SFC have launched their respective pilot schemes to provide a confined regulatory environment for businesses to conduct their operation using insurtech/fintech applications. - **Fast track for applications for virtual insurers** – This is an expedited and streamlined process for new applications for authorization of new insurers, which would own and operate solely digital distribution channels, without the use of any conventional channels involving agents, banks or brokers. - **Insurtech Facilitation Team** – The IA has established an Insurtech Facilitation Team to enhance communication with businesses involved in the development and application of insurtech in Hong Kong and provide a platform for exchanging ideas on innovative insurtech initiatives among key stakeholders. - **Fintech Contact Point** – The SFC has established the Fintech Contact Point to enhance communication with businesses involved in the development and application of fintech that intend to conduct regulated activities in Hong Kong. - **Fintech Facilitation Office** – The HKMA’s Fintech Facilitation Office acts as an initiator of industry research in identifying potential applications and risks of fintech solutions. ■ Policy views – The Hong Kong government has been supportive of the development of fintech/insurtech in Hong Kong and has dedicated resources to promoting Hong Kong’s advantages in fintech, refining the regulatory regime to facilitate the sector’s development, and improving fintech infrastructure. For example, the HKMA is working with the People’s Bank of China to develop a one-stop platform to allow eligible financial institutions and technology firms to conduct pilot trials of cross-boundary fintech projects concurrently in Hong Kong and the Mainland.
INDONESIA	There is currently still no specific regulation that specifically deals with insurtech in Indonesia. However, the Indonesian government has acknowledged and supported the involvement of technological aspects in various business sectors in Indonesia (including the insurance sector). This is evidenced by the issuance of several regulations supporting fintech activities since 2016, such as OJK regulations on peer-to-peer lending platform operations, OJK regulation on financial digital innovation in the financial services sector, and Bank Indonesia regulation on payment service providers. Further, in 2018, the OJK issued a regulation on financial digital innovation in the financial services sector. Under the regulation, insurance (e.g., digital distribution) is included in the scope of digital finance innovation. This regulation provides the general legal framework for digital financial innovation, the types of innovation covered and OJK’s regulatory sandbox for businesses utilizing digital financial innovations.

02 Regulatory Environment for Innovation

What is the attitude and what are the policy views of the regulator in relation to insurtech (if any)? (cont'd)

JAPAN

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 fintech/ insurtech trend and will work towards an environment where 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 (together with the Financial Administration Policy for 2015-2016, the "**Financial Administration Policy**"). Pursuant to 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 established the Expert Panel on FinTech Venture in April 2016 to discuss the desirable environment for the development of fintech. The FSA also established the FinTech Innovation Hub in order to identify regulatory and technological issues and address them in an integrated manner.

The METI is also supportive of the introduction and promotion of fintech-/insurtech-related businesses to the Japanese market. The METI has been holding a series of Study Group on the Integration of Industry, Finance and IT ("**Study Group**") meetings since October 2015. From 21 April 2016 up to 23 May 2016, the METI sought public comments on 11 agenda items relating to fintech. Since 1 July 2016, the METI started holding a series of meetings of the Review Committee for Issues and Future Direction of FinTech ("**FinTech Review Committee**"). The METI consolidated the main points of the discussions of the FinTech Review Committee and issued a final report titled "FinTech Vision" in May 2017.

MALAYSIA

The regulators have been positive, and they 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.

Further, in May 2021, the SC and the UN Capital Development Fund (**UNCDF**) launched the FIKRA Islamic Fintech Accelerator Programme (**FIKRA**), with the objective of further enhancing the Islamic capital market ecosystem by identifying and scaling innovative fintech solutions in Malaysia. FIKRA will connect innovative start-ups through a collaborative environment for mentors, investors and industry enablers, along with relevant regulatory guidance, primarily through a three-month accelerator program.

02 Regulatory Environment for Innovation

What is the attitude and what are the policy views of the regulator in relation to insurtech (if any)? (cont'd)

PHILIPPINES	Regulators encourage the introduction of InsurTech products and services in the Philippines. In 2020, the Insurance Commission released guidelines on the adoption of a regulatory sandbox framework, a controlled environment system that allows a small scale and live-testing of technical innovations for Insurance Technology (InsurTech) Innovations. In creating the Regulatory Sandbox, the Insurance Commission aims for the improvement and enhancement of the insurance business while ensuring that the interests of the insuring public are protected. The Insurance Commission likewise promoted digital payments as part of Insurance Technology, and encouraged its adoption in insurance transactions. They recognize the immense benefit the insurance sector will derive from developing InsurTech as the insurance sector has been a traditional industry and embracing technology in the sector has been at a slower pace compared to other financial industries.
SINGAPORE	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: ▪ Funding – There are currently various funding schemes for fintech/insurtech-related innovations. In particular, the Financial Sector Technology & Innovation scheme (**FSTI**), valid until March 2023, is aimed at growing the fintech/insurtech ecosystem in Singapore by funding the establishment of innovation labs (50% co-funding on qualifying roles for a period of 24 months for each qualifying professional headcount's basic monthly salary); institutional-level projects (up to 50% of level of funding support, capped at SGD1 million); and industry-wide initiatives (up to 70% of level of funding support for qualifying expenses). 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. ▪ Support – 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 (**SFF**) is a good example of Singapore's commitment to promote itself as a fintech/insurtech hub. The sixth edition of the SFF, with the theme "Web 3.0 and its impact on financial services," concluded on 12 November 2021 and attracted 60,000 attendees, representing a 33% year-on-year growth. At the sixth SFF, MAS and partner agencies announced new digital efficiencies and benefits to the financial sector, including the National Artificial Intelligence Programme in Finance to build deep AI capabilities within Singapore's financial sector to strengthen customer service, risk management, and business competitiveness; the second phase of the Singapore Financial Data Exchange (SGFinDex), allowing individuals to now view information on their investment holdings at The Central Depository as part of their consolidated financial position; the Sandbox Plus enhancement to the MAS FinTech Regulatory Sandbox framework, to further catalyze financial innovation and FinTech adoption; and Retail Central Bank Digital Currency (CBDC) paper outlining MAS' preliminary assessment of the economic case for a retail CBDC in Singapore, and its potential implications for financial stability and monetary policy. ▪ Policy views – 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 and enable experimentation of technology innovation to deliver financial products and services. The Regulatory Sandbox, which is fully bespoke, was enhanced with Sandbox Express in 2019 to provide firms with a faster option for market testing in pre-defined environments. Sandbox Plus took effect on 1 January 2022, with three enhancements to provide more effective one-stop assistance for firms looking to introduce innovative products and services that are regulated by MAS: (i) expanded eligibility criteria to include early adopters of technology innovation; (ii) streamlined application with financial grant for first movers of technology innovation; and (iii) eligible applicants allowed to participate in a platform for deal-making opportunities. Sandbox Express will currently be available specifically for insurance brokers, recognized market operators, and remittance businesses.

02 Regulatory Environment for Innovation

What is the attitude and what are the policy views of the regulator in relation to insurtech (if any)? (cont'd)

SINGAPORE (cont'd)	Developing expertise – The MAS has also set up the Financial Technology and Innovation Group within the MAS comprising three divisions (two of which — the Payments & 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.
TAIWAN	To engage fintech/insurtech innovation by the financial institutions, the FSC adopted the following policies: ■ Allowing the 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. ■ Promoting fintech/insurtech development (a) Financial Technology Development Policy White Paper – Published in January 2015, the white paper outlines Taiwan's fintech blueprint, policy goals and strategies in view of international trends and the current domestic situation. (b) Publishing FinTech Development Roadmap – On 27 August 2020, the FSC announced its action plans for 2021-2023, focusing on eight dimensions: (1) one-stop service; (2) data sharing among different entities (phased implementation), including insurance companies and financial institutions (The FSC has released detailed data sharing guidelines on 23 December 2021); (3) fintech compliance; (4) building fintech capacity; (5) digital infrastructure; (6) fintech ecosystem; (7) global network; (8) regtech. (c) On 19 March 2020, the FSC approved a trial application for an insurtech sharing platform supported by blockchain and other innovative technologies filed by 11 life and non-life insurance companies in Taiwan. Through this platform, a policyholder can file claims/make changes in policyholder information with multiple insurers with a single submission instead of contacting each insurer individually. After the six-month trial, the FSC further approved the official launch of the insurtech sharing platform in January 2021. Additionally, the platform is working on e-policy retention with the usage of digital signatures, timestamps, and blockchain storage, which will ensure that e-policies are retained in their entirety and kept updated. If any dispute arises over the authenticity of the insurance policy, this e-policy can be used as evidence provided by an independent third party. (d) On 16 March 2022, the FSC held a meeting regarding the pure digital insurance and invited multiple industry players to discuss their policy for the opening of this new insurance license and the proposed regulations/eligibility requirements. As announced by the FSC, one of the biggest differences in the traditional insurance business and the pure digital insurance is that the latter's product line will focus on innovative insurance policies. (e) Promoting the e-payment ratio multiplication five-year plan – To enhance the efficiency of payments, lower 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 domestic e-payments. Through both the government and private sectors, and the combination of finance and technology, the ratio of e-payments will double in the next five years. (f) Encouraging insurance companies to design innovative products such as usage-based insurance, using big data,

02 Regulatory Environment for Innovation

What is the attitude and what are the policy views of the regulator in relation to insurtech (if any)? (cont'd)

THAILAND	The regulators encourage fintech/insurtech innovation in the following ways: ▪ On the insurance side, the Office of Insurance Commission introduced regulations in the recent years to facilitate change toward a more digital-focused business approach. The commission also established the Center of Insurance to support insurtech and innovation. The fourth five-year insurance development plan (2021–25) focuses on promoting digital insurance and strengthening the local insurance industry by enhancing the insurance ecosystem and relaxing some regulations to facilitate business competition and expansion. ▪ Insurance Regulatory Sandbox – In May 2021, the commission launched a new notification on the insurance regulatory sandbox to promote the innovation and allow applicants to experiment with innovations within a more flexible regulatory requirement as deemed appropriate by the commission. The commission also introduced a sub-regulation on product innovation and a tailor-made sandbox that allows insurers to design more innovative products. ▪ Crowdfunding – Crowdfunding, an alternative means of raising funds by private and public companies, by issuing shares or debentures via an online platform, is regulated under the Notification of the Capital Market Supervisory Board No. TorJor, 21/2562 re: Regulations on the Offering of Securities via Crowd Funding Platform Operators. In providing the services, the Crowdfunding Platform Operator is subject to certain requirements, such as having systems in place for the safekeeping of funds, data access, identifying and authenticating the users of the portal and their qualifications, including suitability assessment for investors. The regulations also prescribe, among other things, qualifications of the private or public company intending to raise funds through the portal, types of qualified investors and the investment limit, and types of debentures that can be issued through the Crowdfunding Platform Operators, etc. ▪ Payment system law – The Payment Systems Act, B.E. 2017 (2560) (the "PSA"), outlines the licensing and regulatory requirements for payment systems and payment services in Thailand, in place of the previous payment law. Under the PSA, there are three categories of regulated activities: (i) highly important payment systems (such as BAHTNET (Bank of Thailand Automated High-value Transfer Network) and ICAS (Imaged Cheque Clearing and Archive System) operated by the BOT); (ii) regulated payment systems; and (iii) regulated payment services. ▪ Others – There will be continued developments in other laws and regulations relevant to the operation of fintech/insurtech businesses such as anti-money laundering laws and exchange control laws, KYC laws and draft law on the operation of digital platform.
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 approvals and licenses. ▪ Developing the corresponding legal framework for fintech activities in Vietnam – To keep up with the development of fintech in Vietnam, regulators have gradually improved and updated the legal framework, in consideration of developments in fintech/insurtech activities, including regulations on e-commerce activities and intermediary payment services. ▪ In relation to the insurance industry, Vietnamese laws do not provide for insurtech in particular, but there are general regulations supporting the application of technology in designing and distributing insurance products. Specifically, under the recently released new draft insurance business law, the regulator proposed a section on the application of technology in insurance and distribution of insurance products over the internet. ▪ Additionally, the Government has been preparing various draft regulations that relate to insurtech and may promote the application of technology in insurance, including the draft law amending the law on e-transactions (e.g., on the conditions for secured e-signatures); the first-ever draft decree on personal data protection (e.g., on the registration of data processing and conditions of cross-border data transfer); the draft decree guiding the cybersecurity law (e.g., on data localization); and the first-ever draft decree on electronic personal identification and verification (e.g., on the verification methods). ▪ Supporting and funding – Vietnamese authorities are aware of the rapid development of fintech/insurtech activities 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 a more conservative view toward technology development in the insurance, financial and banking sectors. For instance, the SBV specifically disallows all use of virtual currency, including Bitcoin, as a payment method in Vietnam.

03 Regulatory Environment for Innovation

What are the licenses required?

CHINA	Depending on the specific activities involved, the following licensing and/or regulatory requirements may be triggered for: ▪ providing service through the internet: license for profitable Internet information service or recordal for non-profitable Internet information service ▪ conducting insurance-related business: licenses for insurer, insurance agency or insurance broker ▪ conducting Internet payment services: license for payment service
HONG KONG	The licenses required will depend on the specific activities contemplated. We recommend seeking the advice of local counsel. In brief: ▪ Designated retail payment systems – The HKMA does not operate a licensing system for RPS. However, for an RPS that 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 to 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) (SFO) 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: (a) For patents: http://www.ipd.gov.hk/eng/applicants/patents.htm (b) For trademarks: http://www.ipd.gov.hk/eng/applicants/trademarks.htm) ▪ Virtual assets exchange – Under the existing SFC's voluntary opt-in regime, a firm that operates a virtual asset-trading platform in Hong Kong offering trading of at least one security token may apply for a license from the SFC pursuant to the SFO. It is proposed that a new regulatory regime will be introduced under which SFC's license is mandatorily required to operate any virtual asset exchange pursuant to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) to be amended.

03 Regulatory Environment for Innovation

What are the licenses required? (cont'd)

HONG KONG (cont'd)

See also the following sandbox schemes for insurtech/fintech:

- IA Insurtech Sandbox enables authorized insurers to experiment with innovative insurtech and other technology applications in a controlled environment to demonstrate that the relevant insurtech application broadly complies with the supervisory requirements of the IA.
- The HKMA Fintech Supervisory Sandbox allows banks and their partnering technology firms (tech firms) to conduct pilot trials of their fintech initiatives involving a limited number of participating customers without the need to achieve full compliance with the HKMA's supervisory requirements.
- The SFC Regulatory Sandbox provides a confined regulatory environment for qualified firms to operate regulated activities under the SFO before fintech is used on a fuller scale.

Please note that the foregoing links may be updated from time to time. We recommend checking with local counsel for updates before relying on the above information.

INDONESIA

The licenses required will depend on the specific activities contemplated, among others:

- Insurance – In the absence of a specific regulation on insurtech, no specific license is required if an insurance company sells an e-policy. In any case, an insurance company must obtain a business license from the OJK.
- 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. 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.

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 a license from the OJK.
- Peer-to-peer lending – Peer-to-peer lending activities require a license 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.

03 Regulatory Environment for Innovation

What are the licenses required? (cont'd)

JAPAN

The licenses required will depend on the specific activities contemplated. We recommend seeking the advice of local counsel as it is difficult to identify under which regulations a particular activity should be under. We set out below an 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**") stipulate 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 as well as products that are substantially the same as the other companies' existing products shall be, in principle, reviewed within 45 days.
- Insurance broker business. 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.
- Financial services broker business. Depending on the scope of brokerage business, registration as a financial services broker who can deal with banking, money lending, securities and insurance business may be required. The criteria to be registered are specified under the relevant provisions in the Act on the Provision of Financial Services. The standard processing period designated under the relevant regulations is 60 days.
- Accepting deposits. A license may be required in order to accept deposits from customers. 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 fifth bullet point 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 fifth bullet point 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, 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. 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, 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.

03 Regulatory Environment for Innovation

What are the licenses required? (cont'd)

MALAYSIA	The licenses required will depend on the specific activities contemplated. The relevant required licenses may include the following: ▪ Banking or insurance licenses and approvals for other approved businesses – No person may carry on banking (including digital banking) or insurance businesses or any other approved businesses such as the operation of a payment system, issuance of a designated payment instrument, money-broking businesses or financial advisory businesses without a license or 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 (including fund management companies that undertake discretionary portfolio management by incorporating innovative technologies (robo-advice)), 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. ▪ 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 (including e-moneylending) must be licensed by the Ministry of Housing and Local Government, unless exempted. ▪ Money services license – Any person engaged in 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 any objections are raised to such registrations, it may take between 1 and 1.5 years to register a trademark and five and six 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 five and six years, it generally takes three to six 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.
PHILIPPINES	Fintech products/services relating to e-money and remittance services (including virtual currency exchange systems), that are used for the digital payments in insurance transactions are required by the Insurance Commission to obtain a license or authority from relevant government authorities, such as 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, financial services licenses 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.

03 Regulatory Environment for Innovation

What are the licenses required? (cont'd)

PHILIPPINES (cont'd)	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. For patents, information is available at 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 For trademarks, information is available at http://info.ipophil.gov.ph/dev/services/trademark/application-process-flow-chart
SINGAPORE	The licenses required will depend on the specific activities contemplated. We recommend seeking the advice of local counsel. In brief: ▪ Financial advisers – The Financial Advisers Act 2001 (**FAA**) regulates the arranging of any contract of insurance in respect of life policies, other than a contract of reinsurance. The FAA licensing framework is technology agnostic and applicable to digital advisers. Note that the relevant regulatory framework applicable to a digital adviser would depend on the operating model of, and specific activities carried out by, the digital adviser. Digital advisers who merely advise and assist in passing on their clients' buy or sell orders to brokerage firms for execution will be required only to hold a Financial Advisers license under the FAA. Digital advisers who rebalance their clients' portfolios are deemed to be conducting fund management activities under the Securities and Futures Act 2001 and will be required to hold a Capital Markets Services license in fund management unless otherwise exempted. ▪ Payments regime – The Payment Services Act 2019 (**PSA**) and related regulations and MAS Notices set out the applicable licensing criteria and ongoing business conduct requirements for providers of those payment services, which MAS has identified as posing sufficient risk to warrant regulation, and where such risks are crucial to address, in order to build a simple, secure, and accessible payments ecosystem. This includes new payment services enabled by evolving technology, which fall outside of the existing regulatory frameworks despite presenting risks to the system as a whole. The PSA regulates all entities providing any type of payment service in Singapore, including money changing, account issuance, domestic money transfer, cross border money transfer, merchant acquisition, e-money issuance and digital payment token (**DPT**) services. Providers of such payment services will be required to be licensed as a Standard Payment Institution license, with a Major Payment Institution license and/or a Money Changer license. Where digital currencies are considered DPT, the DPT service providers will be subject to licensing requirements under the PSA and be required to put in place policies, procedures and controls to address AML/CTF risks. ▪ 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 crowdfunding and FAQs on lending-based crowdfunding. ▪ 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.

03 Regulatory Environment for Innovation

What are the licenses required? (cont'd)

SINGAPORE (cont'd)	■ 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) For 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. We recommend checking 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: ■ Insurance business – Currently, there are two types of insurance licenses available in Taiwan: non-life insurance and life insurance. The insurer holding a non-life insurance license may sell fire insurance, marine insurance, land and air insurance, liability insurance, bonding insurance, and any other type of insurance approved by the Taiwan regulator, the Insurance Bureau. The insurer holding a life insurance license may sell life insurance, personal injury insurance, health insurance, and annuities. Generally, an insurer is not allowed to engage concurrently in non-life insurance and life insurance under Taiwan laws. The exception is that a non-life insurer may be allowed to sell personal injury insurance and health insurance after obtaining approval from the Insurance Bureau. Any non-life insurer that intends to apply for regulatory approval should meet the eligibility requirements under the Regulations Governing Non-Life Insurance Enterprises Engaging in Injury Insurance and Health Insurance. ■ Insurance agency/broker business – The role of the insurance broker is different from that of the insurance agent. An insurance broker is a person/entity who negotiates insurance contracts with the insurers or provides related services based on the interests of the insured, while insurance agents operate the business on behalf of insurance companies and are ultimately managed by the insurance companies. Therefore, these two kinds of businesses are subject to different sets of regulations. Anyone who wishes to engage in the insurance agency business is required to obtain an insurance agent license. The criteria are specified under the relevant provisions of the Regulations Governing Insurance Agents. On the other hand, anyone who wishes to engage in the insurance broker business is required to obtain an insurance broker license. The criteria are specified under the relevant provisions of the Regulations Governing Insurance Brokers. ■ 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 online/and online to offline transaction; (ii) stored-value services; and (iii) domestic and cross-border fund transfer. ■ Remittance business – If anyone wishes to conduct a 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).
THAILAND	The licenses required will depend on the activities contemplated. We recommend seeking the advice of local counsel. Key licenses for insurtech operations in Thailand include insurance license (life/non-life), insurance brokerage license (life/non-life/reinsurance), foreign business license or foreign business certificate, and other financial-related business licenses, such as: ■ financial institution license (commercial bank, credit foncier company, finance company) ■ personal loan license ■ nano-finance license

03 Regulatory Environment for Innovation

What are the licenses required? (cont'd)

THAILAND (cont'd)	■ pico-finance license ■ payment service license ■ 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 ■ digital asset business license (namely digital asset exchange, digital asset broker, digital asset dealer, digital asset fund manager, digital asset advisor) ■ license for direct sale and direct marketing ■ commercial registration ■ In the future, notification for the operation of digital platform (currently a draft Royal Decree).
VIETNAM	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.

04 Regulatory Environment for Innovation

Is the use of telematics and/or biometrics regulated?

CHINA	Telematics services are regulated under several regulations and administrative measures, such as the Regulation on Telecommunications of the P.R.C. (Order No. 291 of the State Council of the P.R.C.) and the Measures for the Administration of Telecommunications Business Licensing (Order No. 42 of the Ministry of Industry and Information Technology). Use of biometric data such as finger print is now under the regulation of the Personal Information Protection Law of the P.R.C. ("**PIPL**"). According to Art. 28 of the PIPL, biometric data are sensitive personal information, which cannot be processed unless there are specific purposes and sufficient necessity and strict protective measures are taken. For financial industry, the People's Bank of China promulgated the Personal Financial Information Protection Technical Specification (JR/T 0171-2020), which contains practical standards for biometric data protection.
HONG KONG	The PCPD has issued the "Guidance on Collection and Use of Biometric Data" 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) (**PDPO**). 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.
INDONESIA	There is no specific regulation regarding telematics and biometrics in Indonesia. The use of telematics and biometrics in Indonesia 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 express consent from the data owner/customer.
JAPAN	There are no specific regulations for the use of telematics. However, any insurance product that uses 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 Act on Protection of Personal Information (**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.

04 Regulatory Environment for Innovation

Is the use of telematics and/or biometrics regulated? (cont'd)

MALAYSIA	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. In June 2020, BNM issued the Electronic Know-Your-Customer (**e-KYC**) Policy Document to set out the minimum requirements applicable to financial institutions in implementing e-KYC customer identification and verification, which, amongst others, mandates the use of biometric technology to verify a customer's identity against their government issued identity document in offering the designated financial products (if e-KYC is adopted). Further, depending on how such technology is used, other areas of regulation (for example, telecommunications or pharmaceuticals) may apply.
PHILIPPINES	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).
SINGAPORE	MAS supports the use of technology by improving the customer onboarding experience while adequately assessing and managing AML/CFT risks and has issued in 2018 guidance to financial institutions (**FI**) on use of non-face-to-face (**NFTF**) verification measures such as MyInfo, which allows users of Singpass (a digital identity) to manage their personal data and pre-fill forms, with their consent, in digital services transactions. Where identity is obtained electronically through other NFTF means, the FI should apply additional checks to mitigate the risk of impersonation, such as using technology solutions including, but not limited to, biometric technologies (e.g., fingerprint or iris scans, facial recognition), which should be linked incontrovertibly to the customer.
TAIWAN	Except for the Personal Data Protection Act, there are no specific regulations for the use of telematics on its own. The biometrics used in the insurance industry will be subject to Article 5 of the Rules Governing the Use of the Innovative Technologies by the Insurance Industry. Furthermore, if a financial institution (including an insurer) provides any services that involve the use of biometrics, and where the said financial institution may process the data from clients, the financial institution is required to abide by the Regulations Governing Security Measures of the Personal Information File for Non-government Agencies Designated by the Financial Supervisory Commission. Additionally, insurance companies should ensure that such use is compliant with any existing regulations (e.g., the outsourcing regulations) or conduct of business requirements.
THAILAND	There are no specific regulations for telematics or biometrics use. Insurance companies should ensure compliance with any existing regulations. If telematics and/or biometrics are part of a new business or product model, insurers would generally need to ensure the compliance with regulated elements under the Insurance Acts such as products approval, premium approval, or claim process. Depending on how the technology is used, other areas of regulation may need to be considered i.e., data privacy, telecom or pharmaceuticals. Any insurance company that engages in an electronic transaction shall be subject to the Secure Method Royal Decree issued under the Electronic Transactions Act (the E-Transactions Act), which requires a strict application of information technology security.
VIETNAM	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).

05 Regulatory Environment for Innovation

Does the regulator offer special benefits to insurance providers that specialize in using insurtech innovations?

CHINA	The People's Bank of China mentioned in the Fintech Development Plan (2022-2025) to offer more policy and funding support for fintech development. In addition, many local governments have published supportive policies and offer special benefits for fintech companies, such as awards and subsidies for registration and technological development, tax credits, funding support, talent incentives
HONG KONG	The IA has launched the Fast Track where virtual insurers that own and operate solely digital distribution channels may apply for authorization under an expedited and streamlined process. Applicants for Fast Track authorization must possess an innovative and robust business model, while being able to satisfy all prevailing regulatory requirements on solvency, capital and local assets requirements. The IA has also launched the Insurtech Sandbox, which enables authorized insurers to experiment with innovative Insurtech and other technology applications in a controlled environment to demonstrate that the relevant insurtech application broadly complies with the supervisory requirements of the IA.
INDONESIA	No special benefits are specifically given to insurers that specialize in using insurtech innovations, given the lack of a regulatory framework that deals specifically with insurtech matters.
JAPAN	Although there are several governmental subsidies for introducing information technologies (mainly for small and mid-sized entities), there do not seem to be special benefits to insurance providers that specialize in using insurtech innovations.
MALAYSIA	In January 2022, BNM has issued a Discussion Paper on the Licensing Framework for Digital Insurers and Takaful Operators (**DITOs**) ("**DITOs Discussion Paper**") that sets out a proposed framework for the DITOs, i.e., an insurance business or takaful business that is carried on wholly or almost wholly through digital or electronic means. Pursuant to the DITOs Discussion Paper, regulatory flexibilities are proposed to be awarded to DITOs during their foundational phase, which include: (a) a lower minimum paid-up capital; and (b) flexibilities on prudential and business conduct requirements that are proportionate to the level of risks presented.
PHILIPPINES	While the Insurance Commission encourages the development and adoption of insurtech in the Philippine market, there are currently no special benefits given to insurance providers that specialize in using insurtech innovations.
SINGAPORE	Singapore-based Life Insurance and General Insurance agencies with less than 200 appointed representatives and employees will be eligible to apply for the Digital Acceleration Grant from 1 October 2021 to 31 December 2021 for projects which contribute to improvements in productivity, efficiency, risk management, operational resilience, or customer service. MAS will offer 80% co-funding of qualifying expenses listed below, capped at SGD 120,000 per entity, for the duration of the scheme.

05 Regulatory Environment for Innovation

Does the regulator offer special benefits to insurance providers that specialize in using insurtech innovations? (cont'd)

TAIWAN	Generally no. The FSC encourages insurance companies to apply for new business with insurtech innovations according to related rules (e.g., Guideline for Trial Application in the Insurance Industry), but the FSC does not offer special benefits to them.
THAILAND	Besides allowing insurers and insurtech firms to participate in the insurance sandbox to test their new innovations, the OIC currently does not offer special benefits to insurance providers that specialize in using insurtech innovations.
VIETNAM	No special benefits to insurance providers that specialize in using insurtech innovations. Instead, the Government offers benefits to innovative startups in general. Under the Government's current project for supporting the innovative and creative startup ecosystem towards 2025 (Decision No. 844/QD-TTg dated 18 May 2016), the key benefits include (i) establishing a national creative and innovative startup portal; (ii) establishing local supporting hub, (iii) establishing individual investment network and risky investment fund network, (iv) funding for training activities, (v) funding for developing supporting technical infrastructure, and (vi) improving regulatory framework for promoting investment in innovative and creative startups.

Data Privacy, Technology and Risk Management

06 Data Privacy, Technology and Risk Management

Are there any laws governing big data, including the collection, use, storage, disclosure and transfer of personal data?

CHINA	The PIPL establishes a comprehensive framework governing any collection, storage, utilization, processing, transmission, provision, publication and deletion of personal data. Under the PIPL, personal data shall be processed under the principles of legality, legitimacy, necessity and good faith, for explicit and reasonable purposes, in manners that have the minimum impacts on individuals' rights and interests. The collection of personal data shall be limited to the minimum scope to fulfil the purpose of processing. In addition, the processing of personal data shall be open and transparent and the rules, purposes, means and scope of processing shall be explicitly disclosed. Data processors shall take technical and other necessary measures to ensure the confidence and safety of personal data. Personal data processors shall also comply with relevant laws such as the Civil Code, the Criminal Law, and the Consumer Protection Law. For insurtech companies, the Personal Financial Information Protection Technical Specification (JR/T 0171-2020) issued by the People's Bank of China can serve as a practical guidance. The Implementing Measures of the People's Bank of China for Protection of Financial Consumers' Rights and Interests (Order No. 5 [2020] of the People's Bank of China) sets out requirements on protection of personal information of financial consumers.
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 and is based around six data protection principles (**DPPs**): ▪ DPP 1—purpose and manner of collection of personal data ▪ DPP 2—accuracy and duration of retention of personal data ▪ DPP 3—use of personal data ▪ DPP 4—security of personal data ▪ DPP 5—information to be generally available ▪ DPP 6—access to personal data 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 also need to ensure that their dealing with personal data does not contravene any business conduct requirements. For example, under the current regulatory regime for insurance intermediaries, 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.
INDONESIA	Indonesia does not have a regulation that deals specifically with big data. Currently, the main regulations on data privacy in Indonesia are: (i) Law No. 11 of 2008 on Electronic Information Transaction, as amended by Law No. 19 of 2016 ("**EIT Law**") (ii) Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("**Regulation 71**") (iii) Minister of Communications and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("**MOCI Regulation 20**") Under Article 1 (29) of Regulation 71, personal data means any individual data that is identified and/or can be identified on its own or combined with other information, whether directly or indirectly, through electronic and/or non-electronic systems. As Law No. 11 of 2008 on Electronic Information and Transactions (as amended, "**EIT Law**") and Regulation 71 regulate electronic transactions, they only regulate data protection issues related to electronic transactions.

06 Data Privacy, Technology and Risk Management

Are there any laws governing big data, including the collection, use, storage, disclosure and transfer of personal data? (cont'd)

INDONESIA (cont'd)

Under Article 14 of Regulation 71, the electronic system provider (Penyelenggara Sistem Elektronik) is obliged to implement personal data protection in processing personal data, as follows:

- Collection of personal data must be done limitedly and specifically, legally, fairly and to the knowledge and approval of the personal data owner
- Personal data processing must be done in accordance with its purpose.
- Personal data processing must be done by guaranteeing the rights of the personal data owner.
- Personal data processing must be done accurately, completely, not misleadingly, up-to-date, accountably and taking into account the purpose of personal data processing.
- Personal data processing is carried out by protecting personal data from loss, misuse, unauthorized access and disclosure, as well as alteration or destruction.
- Personal data processing is carried out by notifying the purpose of collection, processing activities, and failure to protect personal data.
- Personal data is destroyed and/or deleted, unless it is still in the retention period in accordance with the requirements based on the provisions of the regulation.

The term "personal data processing" mentioned above includes: (i) collecting; (ii) processing and analyzing; (iii) storing; (iv) revising and updating; (v) presenting, announcing, transferring, disseminating or disclosing; and/or (vi) deleting or destroying.

As a general rule, every personal data processing must fulfill the requirement to have valid and express consent from data owners for one or several specific purposes that have been conveyed to the data owners. Electronic system operators that conduct data processing must provide an Indonesian language consent form to ask for and obtain express consent from personal data owners.

OJK Regulation No. 1/POJK.07/2013 on Consumers Protection in the Financial Service Sector (as amended, "**POJK 1**") and OJK Circular Letter No. 14/SEOJK.07/2014 on Confidentiality and Security of Consumers' Private Information and/or Data ("**OJK Circular Letter 14**") provide 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 provision of that data. Any transfer of consumers' data to any third party can be done only with a 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. OJK Circular Letter 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, Indonesian identity card or stay permits; and shareholders composition.

Data storage

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.

MOCI Regulation 20 requires any personal data processing (including collecting, processing, analyzing, disclosing) to be done with 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 on 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.

06 Data Privacy, Technology and Risk Management

Are there any laws governing big data, including the collection, use, storage, disclosure and transfer of personal data? (cont'd)

INDONESIA (cont'd)	OJK Regulation No. 69/POJK.05/2016 on Insurance and Reinsurance Companies requires 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.) Insurance companies may put their data center and disaster recovery center offshore with prior approval from OJK if the data is used for certain purposes provided in the regulation. Among others, the data is used for an integrated risk management with the parent company, main entity and/or other entities that have the same line of business under the same group company offshore.
JAPAN	The APPI applies to business operators handling personal information databases. 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.
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.
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."

06 Data Privacy, Technology and Risk Management

Are there any laws governing big data, including the collection, use, storage, disclosure and transfer of personal data? (cont'd)

PHILIPPINES (cont'd)

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

Personal data is protected under the Personal Data Protection Act 2012 (**PDPA**). The PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data. The PDPA is administered and enforced by the Personal Data Protection Commission (**PDPC**), the data privacy regulator in Singapore. The PDPA ensures a baseline standard of protection for personal data by complementing sector-specific legislative and regulatory frameworks. It takes into account the following concepts:

- Consent – Organizations may collect, use or disclose personal data only with the individual's knowledge and consent, subject to certain exceptions.
- Purpose – Organizations may collect, use or disclose personal data in an appropriate manner for the circumstances, and only if they have informed the individual of the purposes for the collection, use or disclosure.
- Reasonableness – Organizations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.

The PDPA applies to personal data only. The PDPA defines 'personal data' as all data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the organisation is likely to have access.

The Data Protection Obligations under the PDPA generally do not apply to business contact information.

Data Protection rules are further supplemented by cybersecurity requirements and other regulatory guidance overseen by MAS. This includes technology risk management notices and guidelines, including cyber hygiene requirements for the insurance industry. The MAS's Fairness, Ethics, Accountability and Transparency principles would be relevant to Fintech solutions that utilize AI and data analytics in the provision of their products.

06 Data Privacy, Technology and Risk Management

Are there any laws governing big data, including the collection, use, storage, disclosure and transfer of personal data? (cont'd)

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	Thailand has already published the Personal Data Protection Act B.E. 2562 (2019). The Act has not been enforced yet. The full enforcement of the Act is expected to take place on 1 June 2022. Currently, the most relevant laws relating to data privacy would be the Constitution of the Kingdom of Thailand B.E. 2560 (2017) and the Wrongful Act (Tort) provided under the Civil and Commercial Code of Thailand. Until the Act becomes fully effective, data controllers are required to arrange for personal data security measures, encompassing administrative safeguard, technical safeguard, physical safeguard and access control under the Notification of Ministry of Digital Economy and Society re: Standards of Personal Data Security B.E. 2563 (2020). The data controller is also obliged to notify the personnel, employees, or associated persons of the security measures. They must also raise awareness of the importance of personal data protection for these groups and ensure strict compliance with the prescribed security measures. These obligations are effective until 31 May 2022. After the Act becomes fully effective, there are several key obligations that data controllers must comply with, such as informing the data subject of required information relating to collection, use and/or disclosure of personal data; to identify the necessary purposes and legal basis for collection, use and/or disclosure of personal data; to provide appropriate security measures for preventing unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of personal data; to examine the system for erasure or destruction of the personal data; to take action to prevent the person or legal person to whom the data is provided to from using or disclosing such personal data unlawfully or without authorization; to notify data breach notification; to prepare record of processing activities; to appoint a Representative who is in Thailand and is authorized to act on behalf of the data controller who is not established in Thailand and Data Protection Officer (**DPO**) (if required), and to comply with the data subjects' exercise of their rights, among others.
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. Recently, the Government has been drafting the first-ever draft decree on personal data protection, with key proposals including a broad definition of personal data, categorization of data into basic personal data and sensitive personal data, registration for processing of sensitive personal data, and conditions for cross-border transfer of personal data of Vietnamese citizens.

07 Data Privacy, Technology and Risk Management

Are there any restrictions that could hinder the growth and usage of insurtech by insurance companies under data privacy laws?

CHINA	The introduction of the PIPL strengthens the protection of personal data, which may raise the compliance costs for data processors, especially on the following aspects: ■ Data localization: the PIPL requires that the operator of critical information infrastructure under the Cybersecurity Law of the P.R.C. and data processors that process the personal data up to the number prescribed by the national cyberspace administration shall store domestically the personal data collected and generated within the territory of the P.R.C. This requirement extends to companies operated outside China so long as they process personal data of natural persons who are located within the territory of China for the purpose of providing products or services to natural persons inside China, or analyzing or evaluating the behaviors of natural persons inside China. ■ Cross-border transfer of personal data: In order to transfer the personal data to parties outside the territory of China, the data processors have to 1) pass the security assessment by the national cyberspace administration, obtain the personal information protection certification by a specialized institution, conclude a standard contract formulated by the national cyberspace administration with the oversea recipient, or comply with other requirements provided by laws or regulations, 2) take necessary measures to ensure that the oversea recipients of personal data meet the personal data protection standards provided in the PIPL, and 3) obtain the separate consent from data subjects. ■ Consent and data management: Separate consent is required for processing sensitive personal information, cross-border transfer of personal information, and the change of processing purpose, processing methods and the type of personal information. Data processors shall take necessary technical and administrative measures to keep the personal data in safety and confidence, and take the initiative to delete personal data when the processing is not necessary, legal, or consistent with agreements with data subjects or the term of service, or when the storage period terminates, or the data subjects withdraw consent.
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 processing 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 policy. 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, consent must be very specific. For example, the customer must know and specifically consent to the actual use of that data (such as data analytics). Moreover, every use and processing of personal data must comply with the applicable personal data protection regulations in Indonesia. See the general rule to obtain express consent in response to question 6 above.

07 Data Privacy, Technology and Risk Management

Are there any restrictions that could hinder the growth and usage of insurtech by insurance companies under data privacy laws? (cont'd)

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, there were discussions on whether the APPI would apply to the use of big data. The relevant market players, including insurance companies, therefore 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 (**JFTC**) is aware of the issue regarding domination of big data by large companies. It published a report of its study group, the Review Committee of Data and Competition Policy, on 6 June 2017. The report mentioned the possibility of applying the Anti-Monopoly Act for certain activities such as unfair data collection or data hoarding. On 17 December 2019, the JFTC published the guidelines on application of abuse of dominant bargaining position under the Anti-Monopoly Act for transactions between digital platformers and customers that provide personal information.
MALAYSIA	Yes. 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 their personal data and be able to correct their personal data.
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

07 Data Privacy, Technology and Risk Management

Are there any restrictions that could hinder the growth and usage of insurtech by insurance companies under data privacy laws? (cont'd)

PHILIPPINES (cont'd)

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.

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.
- The PDPA does not provide for a separate regime governing sensitive data but leaves this to be addressed in sector-specific laws that apply concurrently. The PDPA has also issued enforcement decisions that recognize certain categories of personal data to be of a more sensitive nature -- for example, health data and financial data -- and therefore require a higher standard of protection to protect such data from unauthorized access, collection, use, disclosure or similar risks.

TAIWAN

Yes. According to the TPDPA, the Taiwanese government may prohibit an individual/entity from conducting cross-border transfer of 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 when 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 Operations 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).

07 Data Privacy, Technology and Risk Management

Are there any restrictions that could hinder the growth and usage of insurtech by insurance companies under data privacy laws? (cont'd)

THAILAND	The Personal Data Protection Act imposes various obligations to insurtech operators: ▪ an organization (including insurance companies) acting as data controller is required to ensure 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 consent is revoked by the owners of said data (unless there is any restriction on revoking consent), after the retention period ends or the personal data 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. That said, there are certain restrictions on the processing and transfer of personal data under the draft decree on personal data protection. Specifically, the draft decree requires that the processing of sensitive personal data (e.g., biometric data, health condition data, and location data) must be registered with the Personal Data Protection Committee before processing. Further, cross-border transfers of personal data of Vietnamese citizens are subject to some conditions, including the approval of the Personal Data Protection Committee.

08 Data Privacy, Technology and Risk Management

What laws (if any) do insurance companies have to comply with in respect of technology risk management?

CHINA	Insurance companies shall comply with the following requirements imposed by laws and regulations to manage technology risks: ▪ Building and upgrading information infrastructure and security systems: according to Art. 37, 38 and 48 of the Measures for Regulation of the Internet Insurance Business, insurance companies shall equip themselves with appropriate information infrastructures and security systems in accordance with relevant laws and regulations on cybersecurity and data protection, with the help of technological means such as gateway defense, intrusion detection, data protection, and disaster tolerance. ▪ Strengthening internal management: Art. 37 of the Measures for Regulation of the Internet Insurance Business and Art. 27 of the Data Security Law also emphasize on the use of administrative means such as compliance management, emergency preparedness and educational programs to promote effective management of cybersecurity. Art. 29 of the Data Security Law requires to strengthen risk detection, take remedial action when there are data security holes, and take immediate action and report to users and relevant authorities on occurrence of security events. ▪ Managing the risks arising from algorithm and machine learning: Art. 24 of the PIPL provides that in automated decision-making process, data processors shall ensure that the decision-making process is transparent and the result is fair, just and without discrimination. Art. 28 of the Data Security Law also provides that data processing activities shall not violate social morality and ethics. Specifically, in the Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services (Order No. 9 of the Cyberspace Administration of China, the Ministry of Industry and Information Technology of the P.R.C., the Ministry of Public Security of the P.R.C., and the State Administration for Market Regulation), Art. 7 and 8 require internet service providers to establish an algorithm review system to prevent the users' internet addiction, excessive consumption and other consequences that may violate the law and ethics.
HONG KONG	The IA has published the following guidelines that are relevant to technology risk management: ▪ Guideline on the Use of Internet for Insurance Activities (GL8), which applies to authorized insurers and insurance intermediaries in relation to their insurance activities or transactions conducted on the internet. GL8 requires all practicable steps to be taken to ensure that a comprehensive set of security policies and measures that keep up with advances in internet security technologies are in place and that the electronic payment system (for example, credit card payment system) is secure. ▪ Guideline on the Corporate Governance of Authorized Insurers (GL10), which provides that from a corporate governance perspective, the boards of certain authorized insurers will ensure that there are in place a sound internal control system and a comprehensive risk management policy. In particular, it provides that authorized insurers should put in place cybersecurity policies and mitigation measures. ▪ Guideline on Cybersecurity (GL20), which sets the minimum standard for cybersecurity that authorized insurers are expected to have in place and the general guiding principles the IA adopts in assessing the effectiveness of an insurer's cybersecurity framework. The relevant guideline covers areas such as formulation of strategy, governance, risk assessment and response plan to strengthen the insurance industry's resilience in cybersecurity. ▪ Guideline on Enterprise Risk Management (GL21), which sets out the objectives and requirements related to enterprise risk management and the Own Risk and Solvency Assessment, and provides the impetus for insurers to establish effective tools to identify, monitor, manage and mitigate risks. In particular, according to this guideline, authorized insurers should carry out risk identification in respect of cyber risk and put in place a cyber risk policy. From a data privacy perspective, insurers and insurance intermediaries are required to take appropriate measures to protect customer data against unauthorized or accidental access, processing or erasure under the PDPO. The PCPD has also issued guidance/information leaflets on privacy issues in relation to fintech activities and information technology including mobile app development, development and use of artificial intelligence, and cloud-computing.

08 Data Privacy, Technology and Risk Management

What laws (if any) do insurance companies have to comply with in respect of technology risk management? (cont'd)

INDONESIA	Technology risk management of an insurance company is generally regulated under OJK Regulation No. 4/POJK.05/2021 on Risk Management in the Use of Information Technology by Non-Bank Financial Institutions ("**OJK Regulation 4**"). OJK Regulation 4 requires insurance companies to implement an effective risk management in the use of information technology, which includes at least (i) active monitoring by the board of directors and board of commissioners; (ii) sufficient policy and procedure on the use of information technology; (iii) sufficient identification, measurement, control and risk monitoring processes; and (iv) internal control system on the use of information technology.
JAPAN	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.
MALAYSIA	Among others, licensed insurers must comply with the Policy Document on Risk Management in Technology and Guidelines on Data Management and MIS Framework 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.
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. 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.
SINGAPORE	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. The omnibus Financial Services and Markets Bill, introduced in Parliament on 14 February 2022, will allow MAS to issue directions or make regulations on Technology Risk Management and Notices on Cyber Hygiene (Tech-Risk Notices) to any FI or class of FIs. MAS has indicated it will expect FIs to implement relevant security measures for all systems, regardless if they are air-gapped, critical systems or systems that do not directly support regulated activities. As cyber threat actors exploit every possible entry point and move laterally within the FI's network to perform malicious activities, it is inadequate to secure a subset of systems (e.g., critical systems) while leaving the rest (e.g., those used for accounting or human resource management) vulnerable to attack.

08 Data Privacy, Technology and Risk Management

What laws (if any) do insurance companies have to comply with in respect of technology risk management? (cont'd)

TAIWAN	On 6 August 2020, FSC announced its Financial Cyber Security Action Plan, aiming to strengthen the technology risk management of financial institutions. The Financial Cyber Security Action Plan sets out FSC's expectations for its regulated entities regarding cyber resilience for the next four years. FSC's Financial Cyber Security Action Plan sets out three upcoming regulatory changes that insurance companies might have to comply with in respect of technology risk management. First, FSC will promulgate financial institution-specific cyber security guidelines under Zero Trust Architecture. Second, it is expected that the amendment to the Rules Governing the Use of the Innovative Technologies by the Insurance Industry and the Self-Regulations Governing the Information Technology Security in the Insurance Industry will be made on a rolling basis. Third, the FSC will provide guidelines on supply chain risk management, such as risk assessment and financial audit, which aim to enhance oversight over outsourced service providers. However, as of April 2022, there is no clear timeline of when FSC will release the guidelines/amendments mentioned above. According to the Guidelines for Insurance Enterprises 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, licensed insurers 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.
THAILAND	Licensed insurers will need to comply with the Office of Insurance Commission Notification on Criteria, Processes and Conditions on Enterprise Risk Management and Own Risk Solvency Assessment of Life Insurance Companies B.E. 2562 (2019) and the Notification on Criteria, Processes and Conditions on Enterprise Risk Management and Own Risk Solvency Assessment of Non-Life Insurance Companies B.E. 2562 (2019). These new notifications have adopted enterprise risk management in line with the International Association of Insurance Supervisors (IAIS) standard and introduced the categorization of insurance companies into tiers for flexibility in supervising insurer groups. The notifications have been enforced since 2019.
VIETNAM	Insurance companies should comply with the Consumer Protection Law, Information Technology Law, the Law on Network Information Security, the Law on E-Transactions, Anti-money Laundering Law and relevant specific guiding regulations.

09 Data Privacy, Technology and Risk Management

Are there any laws governing cybersecurity or to mitigate cybersecurity concerns?

CHINA	The Cybersecurity Law is the law regulating the cybersecurity. The Cybersecurity Law stipulates a comprehensive regulatory framework on cybersecurity, provides basic cybersecurity obligations on network operators and establishes a cybersecurity review mechanism for network products and services with national security risks. Specifically, Art. 21 requires network operators to establish security policies and procedures, designate network security personnel, monitor network activities and incidents, and keep the archive of network operation log and the backup of critical data. Art. 40 to Art. 50 stipulate requirements on information security, such as personal information protection and preventing cybercrimes and the transmission of illegal information.
HONG KONG	In Hong Kong, cybersecurity is mainly governed by: ▪ PDPO – see questions 6 and 8 above - Further, section 64 provides that a person commits an offence if the person discloses any data subject's personal data that was obtained from a data user without the data user's consent, with an intent to gain, or to cause loss, in money or other property, to the data subject or with an intent to cause a specified harm (e.g., harassment or psychological harm) to the data subject. ▪ Crimes Ordinance (Cap. 200) – for example: - Section 60 makes it an offense for a person without lawful excuse to destroy or damage any property belonging to another (including misuse of a computer). - Section 161 criminalizes access to computers with criminal or dishonest intent (which potentially covers hacking). ▪ Theft Ordinance (Cap. 210) – for example: - Section 2 provides that a person commits theft if they dishonestly appropriate property belonging to another with the intention of permanently depriving the other of it. "Property" includes intangible property such as digital data or electronic files. - Section 16A provides that a person commits the offense of fraud if any person by any deceit and with intent to defraud induces another person to commit an act or make an omission which results in either a benefit for anyone other than the second-mentioned person or in prejudice or a substantial risk of prejudice to any person other than the first-mentioned person. This potentially covers uses of internet services or software to defraud the victims. - Section 23 provides that a person commits blackmail if, with a view to gain for themselves or another or with intent to cause loss to another, they make any unwarranted demand with menaces. Further, Hong Kong authorized insurers should comply with Guideline on Cybersecurity (GL20) – see question 8 above. In Hong Kong, there is currently no statutory requirement on the data users to give notifications to the relevant regulator(s) or the data subjects in case of a data breach incident. Such notification may be made on a voluntary basis and the PCPD has published a "Guidance on Data Breach Handling and the Giving of Breach Notifications" in this regard. For authorized insurers in Hong Kong, according to GL20, in case of a cybersecurity incident, the insurer should report the incident with the related information to the IA as soon as practicable, and in any event no later than 72 hours from detection.
INDONESIA	The EIT Law provides criminal sanctions for unauthorized use of electronic information, among others: ▪ Maximum fines of IDR 600 million to IDR 800 million and/or six to eight years' imprisonment for unlawful access ▪ Maximum fines of IDR 800 million and/or 10 years' imprisonment for interception/wiretapping of transmission ▪ Maximum fines of IDR 2 billion to IDR 5 billion and/or eight to 10 years' imprisonment for the alteration, addition, reduction, transmission, tampering, deletion, moving or hiding of electronic information and/or electronic records

09 Data Privacy, Technology and Risk Management

Are there any laws governing cybersecurity or to mitigate cybersecurity concerns? (cont'd)

INDONESIA (cont'd)	▪ Maximum fines of IDR 12 billion and/or 12 years' imprisonment for the manipulation, creation, alteration, destruction or damage of electronic informa¬tion and/or electronic documents with the purpose of creating an assumption that such electronic information and/or documents are authentic Regulation 71 provides administrative sanctions for violations of personal data protection in the form of written warnings, administrative fines, temporary suspension, blocking of access and/or deletion from lists. MOCI Regulation 20 provides administrative sanctions for violations of personal data protection in the form of verbal warnings, written warnings, temporary suspension of activities and an announcement on the MOCI's website stating that the party has not complied with data protection regulations.
JAPAN	Yes. The Basic Act on Cybersecurity provides the framework of the government's cyber security strategy and basic policies. The Act on the Formation of a Digital Society also requires the government to take necessary measures to ensure cybersecurity. In addition, the APPI, the Unfair Competition Prevention Act, the Penal Code and the Act concerning the Prohibition of Unauthorized Computer Access also provide some obligations and penalties in relation to cybersecurity.
MALAYSIA	There is currently no single cybersecurity law in Malaysia. The regulation of cybersecurity is addressed through various laws in Malaysia, which includes the Computer Crimes Act 1997, the Communications and Multimedia Act 1998, and the Personal Data Protection Act 2010. This will also need to be overlaid with the regulations or guidelines issued by the sectoral regulator, i.e., BNM. Pursuant to the Policy Document on Risk Management in Technology issued by BNM, all licensed insurers are required to comply with, amongst others, the following in order to mitigate cybersecurity concerns: (a) Establish a cyber-resilience framework to ensure, amongst others, operational resilience against extreme but plausible cyberattacks. (b) Establish clear responsibilities for cybersecurity operations. (c) Ensure their technology systems and infrastructure, including critical systems outsourced to or hosted by third-party service providers, are adequately protected against distributed denial of service attacks. (d) Establish clear data loss prevention strategies and processes. (e) Ensure its security operations center has adequate capabilities for proactive monitoring of its technology security posture. (f) Immediately notify BNM of any cyber incidents affecting the institution.
PHILIPPINES	Republic Act No. 10175 or the Cybercrime Prevention Act (**CPA**) punishes acts that undermine the confidentiality, integrity, and availability of computer data and systems (i.e. illegal access, illegal interception, data interference, cybersquatting), computer-related offenses (i.e. forgery, fraud, identity theft), and content-related offenses. The CPA also punishes any other offense committed through and with the use of information and communication technologies one degree higher than that provided for in the law punishing said offense. Republic Act No. 10173 or the Data Privacy Act (**DPA**) likewise provides a heavy responsibility to the Personal Information Controller for personal information under its control and custody even on the hands of third party for processing. The DPA likewise punishes as crime unauthorized access and/or processing of personal information, improper disposal of personal information, and other similar acts to deter improper handling of personal information.

09 Data Privacy, Technology and Risk Management

Are there any laws governing cybersecurity or to mitigate cybersecurity concerns? (cont'd)

SINGAPORE	The Cybersecurity Act 2018 establishes a framework for the protection of critical information infrastructure (**CII**) against cybersecurity threats; the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore; and the regulation of providers of licensable cybersecurity services. The Singapore Computer Emergency Response Team (**SingCERT**), set up by the Cyber Security Agency (**CSA**) to facilitate the detection, resolution and prevention of cybersecurity-related incidents on the internet, has recently issued a list of measures that organizations should adopt to ensure proper cyber hygiene controls are in place and operating correctly. The CSA has also embarked on two new initiatives to enhance the cyber resilience of Critical Information Infrastructure (CII1) sectors and better secure Singapore's cyberspace. These initiatives are: (a) review of the Cybersecurity Act 2018 to update it for the fast-changing digital world – to improve Singapore's cybersecurity posture and support our digital economy and way of life; and (b) update of the Cybersecurity Code of Practice for the 11 CII sectors, including banking and finance, to better deal with new and emerging threats such as ransomware and domain-specific risks such as 5G.
TAIWAN	Yes. Please refer to our responses to Question 8.
THAILAND	Thailand has published the Cybersecurity Act B.E. 2562 (2019) and the subordinate regulation thereunder. The Cybersecurity Act imposes certain obligations on the Critical Information Infrastructure Organization (CII Organization) and/or private entity to prevent or cope with cyber threats. Most provisions are imposed on the CII Organization. Although insurance companies are not categorized as the CII Organization, they are still subject to the obligations applicable to a private entity, such as providing support to competent officials in investigating cyber threats. Compliance obligations vary with each level of cyber threats (i.e., crisis level, critical level, and non-critical level).
VIETNAM	Yes. Vietnam's National Assembly passed the Cybersecurity Law on 12 June 2018, with effect from 1 January 2019. One of the key concerns for enterprises under this law is the data localization requirement, which requires certain entities to store data within the territory of Vietnam. This requirement applies to both local and foreign enterprises, which: ■ Provide services on the telecom network, the internet and value-added services on cyberspace in Vietnam (i.e., Cyberspace Service Providers); and ■ Are involved in the collection, exploitation, analysis and/or processing of personal information, data about service users' relationship and/or the data generated by service users in Vietnam However, detailed guiding regulations, especially on data localization triggering events, are still in the form of a draft decree and are subject to further changes. Pending the issuance of the guiding decree, on 18 February 2022, the MPS issued Official Letter No. 470/BCA-ANKT stating that data localization will not be triggered if enterprises fully comply with the requirements and coordinate with the MPS in providing information for the investigation and handling of related violators.

Asia Pacific Guide to Insurtech Innovation and Utilization

Market Trends

10 Market Trends

What innovations are insurance companies and/or regulators looking at implementing?

CHINA	In the Several Opinions of the State Council on Accelerating the Development of the Modern Insurance Service Industry (No. 29 [2014] of the State Council), the State Council encourages insurance companies to use new technologies such as network, cloud computing, big data, and mobile internet, to promote innovations in marketing channels and service modes. Under the guidance of the former China Insurance Regulatory Commission (now merged into the CBIRC), the Insurance Society of China and Fudan University jointly issued the China Insurtech Development White Paper, and addressed 10 practices concerning the integration of insurance and technologies, including the blockchain, artificial intelligence, internet of things, cloud computing, big data, car networking, autonomous driving, unmanned aerial vehicle, genetic testing and wearable devices.
HONG KONG	Hong Kong is experiencing significant growth in fintech/insurtech markets. As mentioned above, the Hong Kong regulators and government have been supportive in developing Hong Kong as a fintech/insurtech hub and launched a number of initiatives, including the introduction of regulatory sandbox schemes and providing funding/subsidies for fintech and insurtech related trainings and projects. In December 2020, the Hong Kong government launched the "iAM Smart" Platform to all Hong Kong residents free of charge, enabling them to use a single digital identity and authentication method to conduct various online government and commercial transactions. An iAM Smart account will be bound to the personal mobile device of the user and the user can make use of the biometric functions provided by their personal mobile device to authenticate their identities for log-in of online services. iAM Smart also supports digital signing with legal backing under the Electronic Transactions Ordinance (Cap. 553) for handling statutory documents and relevant procedures. The Hong Kong government is looking to more organizations/companies (such as banks and insurance companies) to adopt "iAM Smart." Given the supportive regulatory environment, with the IA putting in place the Fast-Track authorization scheme that expedites authorizations to carry out insurance business solely through digital channels, several virtual insurers have been granted a virtual insurance license. This enables customers to purchase and manage their insurance policies through an entirely digital platform, which is backed by advanced analytics and automation of traditionally manual processes across claims processing, policy management, and customer service. It is foreseen that there will be an upward trend of using digital platforms to distribute insurance products and service the customers in Hong Kong. Further, it is expected that more insurance companies will form partnerships with other businesses to provide innovative products. For example: ▪ Some insurance companies have partnered with genetic testing and digital health companies to provide genetic tests to policyholders. The tests include genetic tests for diet, hereditary health conditions, responses to medication, risk of inherited cancers and preconception screening. Policyholders who have taken the test will have access to an application that will make diet and lifestyle recommendations based on their DNA profile. This can result in effective personalized treatments and preventive actions taken for policyholders. ▪ A Hong Kong virtual insurer partnered with a cryptocurrency exchange to offer insurance for cryptocurrencies that protects clients' cryptocurrencies entrusted to the exchange against risks such as theft and cybersecurity threats. This novel insurance solution that provides digital asset protection for cryptocurrencies may alleviate concerns discouraging potential investors from entering the crypto market. There are also digital platforms that help consumers save time and money by offering a free and easy online market comparison of banking and insurance products.
INDONESIA	In Indonesia, insurtech businesses have recently become more developed in recent past years, especially given the COVID-19 pandemic. This can be seen by the launch of several insurance marketplaces or startups. Although there is no specific regulatory framework for insurtech business, the government is seen to be supportive of and acknowledges the development of fintech and insurtech businesses in Indonesia, as can be seen by, among others, the issuance of OJK Regulation 4.

10 Market Trends

What innovations are insurance companies and/or regulators looking at implementing? (cont'd)

JAPAN	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. Since a non-life insurance company launched in 2018 a "health promotion" insurance product that incorporates a wellness program that rewards policyholders for their health-conscious activities, several insurance companies started to sell similar insurance products. The regulatory sandbox framework was introduced in June 2018 to facilitate realization of innovative technologies and business models. An insurance startup conducted a demonstration experiment in relation to P2P insurance products.
MALAYSIA	As mentioned in question 3 above, BNM has launched the Financial Technology Regulatory Sandbox Framework. Further, BNM, through FTEG has rolled out an initiative called "Fintech Hacks," which allows the public to submit through the BNM website innovative ideas on improvements to the financial services sector by harnessing innovation and technology. In 2019, BNM issued the Exposure Draft on the Insurance and Takaful Aggregation Business Registration Procedure and Requirements, which proposed for the insurance and takaful aggregation business to be regulated by the BNM as a new category of registered business under the FSA. Upon such requirement coming into effect, the insurance and takaful aggregators approved by BNM under the Financial Technology Regulatory Sandbox Framework and persons intending to become registered insurance and takaful aggregators will need to be registered under the FSA to carry out such business. BNM also issued the DITOs Discussion Paper recently. When BNM progresses with this initiative, it is anticipated that there will be a licensing framework (with new licenses to be issued) for digital insurers and takaful operators. This will change the insurance offering landscape in Malaysia.
PHILIPPINES	A life insurance provider in the Philippines, and 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.
SINGAPORE	MAS has proposed support for life insurance and general insurance agencies adopting digital solutions such as: ■ Cloud services ■ Communication and collaboration tools ■ Compliance and KYC tools (including transaction monitoring tools) ■ Customer relationship and engagement tools (including digital customer onboarding, excluding fees for web domains) ■ Data-related services (including data warehousing, data automation, and data analytics) ■ Enterprise services (including HR and accounting systems, excluding email services and internet connectivity fees) ■ Marketing productivity tools (including customer sensing tools, insights generation, excluding advertising and SEO expenses) ■ Office productivity tools (excluding basic software for individual uses) ■ Project management, development and testing tools

10 Market Trends

What innovations are insurance companies and/or regulators looking at implementing? (cont'd)

SINGAPORE (cont'd)	▪ Security-related solutions (excluding anti-virus software for individual laptop/desktop use, firewalls and switch ports, and VPN tokens) ▪ Digital solutions/software to support alternative working arrangements, operational resilience and BCP.
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). On 18 November 2021, the FSC published the ''Directions Governing the Insurance Industry for Engaging in Remote Insurance Sales/Purchases and Other Insurance Services'' to encourage more zero-contact insurance purchases and provision of insurance services during the pandemic. Insurance companies would have to file trial applications with the FSC for engaging in this new business model. Under this new business model, insurers will be allowed to conduct KYC and identity verification and obtain customer consent in purchasing insurance products via video calls. As of February 2022, eight life insurers are already exploring this new business model. According to the FSC, so far, around 30% of new insurance policies have been sold via this new distribution channel. As the need for remote insurance purchases increases, the FSC plans to expand the permissible business scope (e.g., allowing the insurance agent or broker to provide or engage in the sales under the said Directions) by Q3 2022 at the earliest. The expansion is expected to boost the insurance business as the new business model would enable insurers to overcome time and geographic restrictions in sales of insurance products now that customers can purchase insurance anytime and anywhere. In December 2021, the FSC announced its plan for the opening of purely digital insurance, which encourages insurance companies to use fintech and other innovative technologies (e.g., AI, machine learning, big data and blockchain) to design more sophisticated insurance products (such as usage-based insurance for delivery drivers or car rental services) and more convenient consumer services (e.g., using AI in underwriting and adjusting claims, or using blockchain for clients to file claims). On 16 March 2022, the FSC held a meeting regarding pure digital insurance and invited multiple industry players to discuss their policies on the opening of this new insurance license as well as the proposed regulations/eligibility requirements. As of April 2022, the FSC has not yet finalized the proposed regulations for purely digital insurance.
THAILAND	The pandemic has forced insurance players to adapt and explore the use of new technologies to accommodate customers. Changes from physical to online operations have been observed. The shift started with front-end functions such as sales and customer service. There is a need on the part of the regulator and insurance players to use technology and resulting new solutions for back-end functions in the insurance value chain. This is one of the key drivers of a technology-focused initiative under the new Insurance Development Plan. The Office of the Insurance Commission has said that digital transformation will be a key focus in coming years. The potential exists for insurers employing new technologies to be recognized by the commission, giving them the opportunity to push for laxer foreign shareholding rules. The commission first launched a regulatory sandbox in July 2017 to enable insurers, brokers, and fintech/insurtech players to test their innovations. The sandbox process has been updated regularly, with the most recent setup put in place in 2021. Insurers have been keen on participating in the scheme, yet participation is overwhelmingly from top insurance companies due to resource limitations. The commission also tries to leverage the industry's big data players under its control in an effort to protect consumers. The introduction of the official platform that allows consumers to check the status of all insurance policies is an example of these efforts. Many insurance players have debuted new innovations to the market, particularly within automotive and health insurance. Insurance products have been developed to fit into daily lives. New motor insurance products can be activated and deactivated at the customer's will. Health insurance products that monitor customer behavior constantly (and make lifestyle suggestions) are also a new addition. Further innovation is inevitable due to the drastic change in working environment and lifestyle.
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 determine their target customers and business decisions.

11 Market Trends

Have there been fintech/insurtech-related cases (including competition and/or data privacy) in Asia Pacific?

CHINA	Anti-money laundering has been a serious concern for regulators. Many third-party payment platforms were reported to provide fund transfer service for illegal activities such as gambling, prostitution and other crimes. According to the Anti-money Laundering Law of the P.R.C. and the Measures for the Supervision and Administration of Combating Money Laundering and Financing of Terrorism by Financial Institutions (Order No. 3 [2021] of the People's Bank of China), third-party platforms have the duty to detect and prevent money laundering. Recently, it is reported that Wechat Payment violated relevant laws and regulatory provisions on anti-money laundering for failing to verify the identity of users and the source of funds, and providing service for illegal transactions. Wechat Payment may face a record-breaking fine of over 100 million RMB. The leakage of client information in financial institutions have also been a serious problem. In many cases, employees of financial institutions were charged of the offense of infringing personal information for leakage or illegal sale of client information. With respect to competition law enforcement, joint ventures established by traditional financial institutions and internet giants have been investigated for violation of anti-monopoly law. For example, CITIC aiBank is an AI-driven internet bank established by CITIC Bank, an influential bank in China, and Baidu, one of the top internet companies in China. According to the State Administration for Market Regulation, during the process of establishment, CITIC aiBank did not report the concentration of undertakings, which violated the Anti-monopoly Law of the P.R.C.
HONG KONG	There are no specific cases by the financial regulators so far. However, the SFC, HKMA and IA have raised concerns over activities related to virtual assets (**VA**) and virtual asset service providers (**VASPs**) and have published relevant guidance. In particular, the IA has issued a letter entitled "Regulatory Approaches of the Insurance Authority in Relation to Virtual Assets and Virtual Asset Service Providers" on 28 January 2022 reminding authorized insurers of regulatory requirements relating to engagement in VA-related activities or with VASPs. These cover compliance with the Guideline on Enterprise Risk Management (**GL21**), and the potential exposure to investment risks, cyber risks, conduct risks, anti-money laundering and counter-financing of terrorism risks, and risk of offshore clients and compliance with laws outside Hong Kong.
INDONESIA	We are not aware of any fintech/insurtech cases (noting that there are no law reports in Indonesia).
JAPAN	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 involved 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.
MALAYSIA	There are no specific cases by the financial regulators so far.

11 Market Trends

Have there been fintech/insurtech-related cases (including competition and/or data privacy) in Asia Pacific? (cont'd)

PHILIPPINES	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.
SINGAPORE	On 17 March 2016, the Competition Commission of Singapore issued an infringement decision against 10 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 10 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	There are no specific competition/data privacy cases by the financial regulators so far, but below are financial enterprises that have recently been using fintech/insurtech to provide their services for consideration. ▪ How Investech Inc., a newly licensed securities company approved by the FSC in 2021, provides investors with online trading services through its AI investment analysis and calculation system. ▪ Taiwan Life Insurance Company uses AI systems in tandem with the Taiwan National Health Insurance database to conduct data analysis so that customers can accurately manage personal health assessments and risk predictions, and consequently select and purchase the most appropriate insurance policies. ▪ China Life Insurance Company and Hua-Nan Commercial Bank have obtained the FSC's approval on its trial application for engaging in remote insurance purchase backed by biometrics technologies in March 2022. In the future, any retail customer who wishes to purchase China Life's insurance products could use their own mobile to log on to the official website of Hua-Nan Bank and turn on their camera to conduct facial recognition via China Life/Hua-Nan's special biometrics technologies and complete the insurance purchases remotely and easily.
THAILAND	There are no specific cases by the insurance regulator and trade competition regulator so far. With regard to data privacy, as the Personal Data Protection Act is not fully yet effective, there are no specific cases initiated by the data privacy regulator at this stage.
VIETNAM	There are no specific cases by the financial regulators so far.

12 Market Trends

What are the most immediate challenges to insurtech innovation?

CHINA	■ The difficulty to achieve high-quality and swift delivery. With the enhanced technological capabilities, insurance companies put forward higher requirements on technological talents. At present, it is hard to change within a short period the fact that the abilities of developers at most insurance companies are uneven. The business of insurance companies relies more and more on software systems and the demand for software development is accelerating. All insurance companies face the challenge to improve the efficiency of software development and to achieve swift delivery while ensuring the stability of systems. ■ The pressure of operation and maintenance brought by increasing number of systems. With the increasing number of systems and the internet transformation of system architecture, insurance companies are under the pressure of system operation and maintenance. Insurance companies have the urgent needs to build up agile, efficient, and reusable cloud computing platforms, to strengthen their basic capabilities of digitalization, to improve resource efficiency, and to quickly respond to high-concurrency, multi-frequency and high-traffic business scenarios and to scenario-based service requirements. ■ The difficulty to achieve independent technological innovation. The usual causes that limit the development and application of new technology are the risks associated with the technology and technological and promotional obstacles. Faced with the great potential and opportunities in the development of frontier technologies, insurance companies should raise their requirements on technology teams, avoid heavy dependence on external technological resources and effectively promote the application of new technologies.
HONG KONG	■ Complexity of the sector-specific regulatory regime in Hong Kong and the different types of licenses and/or authorization needed ■ Legal uncertainty relating to regulatory activities – Since the IA took over the regulation of insurance intermediaries in September 2019, there has been more stringent regulation over regulated activities and there remains uncertainty as to the application of the regulated activities regime to cyber-activities in practice. The IA has helpfully issued guidance notes on "regulated activities" toward the end of 2021. Having said that, the rapid development of insurtech may still result in grey areas as to whether the non-traditional distribution channels may fall under the definition of regulatory activities and thus the licensing regime. ■ The high costs of development and innovation ■ Cybersecurity – As cyber criminals become more sophisticated, 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. The OJK also has its own regulatory sandbox for businesses that are within the scope of digital financial innovations under OJK regulation. ■ Technology – Local technology may not be sufficient to accommodate the development of fintech products. ■ Customers – Although internet use is becoming more common in Indonesia and Indonesians are more tech-savvy than before, customers may take time to accept fintech/insurtech. Currently, sales of financial products are mostly personal in nature (for example, telemarketing and agents). Customers will need more assurance and time to accept fintech/insurtech services.
JAPAN	■ The delay in digital transformation for both government and corporations ■ Sluggish investment in insurtech companies/startups ■ The lack of skilled personnel who have both financial and technological capacity, and the limited mobility of such skilled personnel

12 Market Trends

What are the most immediate challenges to insurtech innovation? (cont'd)

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 prescriptions 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 skillset to catalyze fintech/insurtech developments in Malaysia are lacking. Guidance will have to be sought from more developed markets.
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 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 cybercriminals become more sophisticated, 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. ■ There is a lack of patent and knowhow to develop fintech. ■ Legislation can hardly catch up with the technological developments. ■ The attitude of the regulator remains conservative.

12 Market Trends

What are the most immediate challenges to insurtech innovation? (cont'd)

THAILAND	■ The regulator's understanding of the entire value chain. Insurtech, innovation, and technology need to be applied throughout, not only the front-end function. ■ Regulations need to address the customers' perspective. At times, the introduction of more stringent regulations hamstrings companies from providing improved customer experiences. Balance is key. ■ Insurtech businesses may not always fall squarely within any particular regulatory regime. The regulatory sandbox approach seeks to mitigate uncertainty, but some legal restrictions that continue to create hurdles for new projects are not easily definable under the paradigm. ■ Limited support for the development and improvement of innovation. ■ The general public has low knowledge and understanding. Innovation developers (a younger demographic) find no room to explore designs and apply innovation. This limits forward mobility. A basic understanding of the insurance business must be fostered among developers. ■ The industry comprises several big players dominating the market. They come with a profound understanding of the business and are extremely active in spotting opportunities for innovation. This makes it difficult for startups to break into the market. If they make a mark at the outset, there is a distinct trend of startups needing to partner with established insurers or eventually selling and exiting the market entirely.
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.

13 Market Trends

What has been, or could be, the impact of fintech/insurtech on the financial services industry?

CHINA	Insurtech is capable of reshaping the ecosystem of insurance industry. It helps the insurance company design more flexible and smart insurance products that caters to the different needs of consumers, optimize business efficiency in the delivery of service, respond to the change of status in a timely manner, and computing and monitor the risk in complex scenarios at a large scale.
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	Fintech/insurtech has become more prominent in Indonesia, ever since the COVID-19 pandemic and will likely continue to grow rapidly given the increasing use of digital service. The growth of fintech/insurtech in Indonesia opens new business opportunities in the financial sector and provides better access to financing for business players.
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 sectors (please refer to question 14 below). 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. In addition, the BNM is expected to approve up to five digital bank licensees in the first half of 2022, which would accelerate the access to finance for the unserved and underserved markets. 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.
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.

13 Market Trends

What has been, or could be, the impact of fintech/insurtech on the financial services industry? (cont'd)

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	Fintech and insurtech will likely spur the development of innovative financial products or services. However, in Taiwan, conventional financial institutions might still play the dominant role in the growth and development of the insurance industry. Start-ups or tech companies might not be able to replace the existing financial institutions or win against the competition in the near future because of the high industry entry barrier and the compliance costs. As such, more fintech startups or tech companies choose to collaborate with traditional financial institutions instead of trying to compete directly with them. On the other hand, some financial institutions also hold an open attitude to the benefit that could be brought by collaborating with fintech startups. ▪ Innovative technology plays a complementary role in enabling financial institutions to offer a wider range of services. ▪ Providing financial services remotely has become the focus of recent discussions due to the COVID-19 outbreak, such as opening a bank account or purchasing insurance remotely.
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. These new trends should be closely monitored. Bigger players need to be more innovative and competition. The entire industry needs to be invigorated. Regulators are being forced to have a better understanding of new innovations and trends in order to catch up with rapid changes, ensuring appropriate regulations can be issued and implemented in a manner that helps regulate new innovations and benefits the general public. Fintech/insurtech innovations could redefine the way the financial services industry is structured. Traditional communications between customers and operators are likely to be reinvented. Innovation would also serve as a key function to make a better connection between customers and the business operators. The development of fintech/insurtech would create opportunity for up-and-coming developers and financial service players. Cooperation within the industry, such as joint ventures, is more likely. Existing players could become key investors in new fintech/insurtech startups. There will also be more opportunities for M&A activities as a way to either expand or protect ongoing businesses.
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.

14 Market Trends

What insurtech trends or disruptions may impact insurance companies?

CHINA	■ Consumers' preference towards online insurance service: More and more consumers opt for online insurance services due to the convenient interaction, transparent price and instant issuance of policy. Online insurance service has great potential to grow continuously with the huge amount of internet users in China. Large internet platforms such as Alipay have turned many users into insurance customers by offering scenario-based insurance products with deep understanding of consumers' behaviors and demands. Insurance companies have to improve the quality of their online service and prioritize consumers' experience to gain competitive advantages. ■ Integration into the digital ecosystems: With the application of Internet of Things, the landscape of insurance business mode may be fundamentally changed. The digital ecosystems built up by internet-connected devices, sensors and activators can transmit huge amount of real-time data and enable immediate and accurate risk assessments. The function of insurance will shift from risk transfer to risk control. With the accurate data of the insured property or human behaviors, insurance companies can design products and price the policy based on the usage of insured property or risky behaviors, which allows consumers to be insured in periodic or occasional situations without entering into long-term coverage. ■ Personalization: Big data and enhanced data analytical abilities enable insurance companies to provide personalized insurance products catering for the narrow needs of consumers. Under the big data analytics, risk selection can be individualized and pricing strategies can accommodate a wide-range fluctuation. More and more personalized insurance products may emerge in the future.
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 such 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 discounts, determining future premiums, etc.). As the use of such analytics may directly affect customers, any incidents of misuse, leakage or improper application of such analytics will pose a reputational risk for the insurer. There is greater adoption of open application programming interfaces (APIs) technology by Hong Kong insurers. Such "open insurance" can facilitate data connectivity between their platforms and their business partners to reach a wider range of potential policyholders for customer acquisitions, policy administration and claim management. Furthermore, this allows the improved use of data sharing, enabling insurers to generate new revenue streams and achieve greater customer personalization.
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 regulations are being updated to adjust to the growing digitalization of the financial industry. 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 with 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.

14 Market Trends

What insurtech trends or disruptions may impact insurance companies? (cont'd)

JAPAN	According to a report prepared by a research institute, the market size of the Japanese insurtech market was expected to expand to JPY 188 billion in FY 2021 from JPY 60 billion in FY 2017. It is even expected to be JPY 280 billion for FY 2023, more than 4.6 times that of the FY 2017 figure. In the past five years, there have been many cross-border and domestic joint ventures incorporated to develop and introduce new insurance products and services using technologies, and this existing trend of insurance companies making significant investments in R&D on products utilizing insurtech is expected to continue.
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 labor-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 risk measures. Meanwhile, 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. The DITOs Discussion Paper also provides that BNM expects licensed DITOs to heavily leverage on digital means for all critical functions, including onboarding, underwriting, distribution, policy servicing and claims processing and payment.
PHILIPPINES	We expect insurance companies partnering with insurtech and technology entities to help them develop their technology and business strategies.
SINGAPORE	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 "aggregator" 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.

14 Market Trends

What insurtech trends or disruptions may impact insurance companies? (cont'd)

SINGAPORE (cont'd)	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, 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.
TAIWAN	As insurtech/fintech continues to evolve, online financial services have become the new choice for consumers. Considering that financial institutions need to conduct KYC, verify consumers' identities and confirm whether they are authorized, there is a need to ensure service security and ease of use from registration and login to transactions. In order to encourage financial institutions and fintech companies to develop and utilize the latest technologies, and to propose applications that will make it easier and more secure for consumers to use digital financial services, FSC plans to conduct a sandbox and business trial with the theme of "Digital Identity Verification and Authorization" in 2022, focusing on four main areas: identity proofing, KYC, authentication and authorization.
THAILAND	Insurance companies are expected to become more involved in various areas of innovation. This will come about as independent efforts or through partnerships with other insurtech operators, in order to create efficient operation models. Insurance product offers, price comparisons between insurance products and policy underwriting, and claims management services are areas with potential. Insurtech and innovation may alter the existing insurance model's use of labor, which is a fixed operational cost. Physical offices and branches will continue to lose foot traffic. Insurers employing insurtech will be better positioned to spot investment opportunities. Insurtech will help improve customers' journey experience, an important point of note for the regulator. Competition between insurance companies to capture this new business opportunity is expected. Insurance companies are likely to be forced to upgrade products to catch up with lifestyles. Close monitoring and research on customer interest and behavior would be the key focus. Operators may also look to invest in venture capital companies that cater to insurtech startups and must also look to younger recruits with the potential to navigate trends successfully.
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. More insurance companies are cooperating with insurtech players to diversify their insurance products and distribution channels and facilitate the development of the insurance market in Vietnam. In particular, electronic transactions will be developed to supersede traditional transactions. In the times of the COVID-19 pandemic and robust technology development, more and more innovative insurance products have been offered completely via online channels (e.g., insurers' websites, mobile applications). We expect that insurers will improve their competitive advantage and bring more benefit to the insurance purchasers as well.

15 Market Trends

Are cryptocurrencies or digital tokens used within insurtech/insurance operations?

CHINA	Except digital RMB or Digital Currency Electronic Payment issued by the People's Bank of China, financial activities concerning cryptocurrencies or digital tokens are illegal in China. Currently, there is no application of cryptocurrencies or digital tokens within insurtech/insurance operation.
HONG KONG	Whilst there are insurance products for digital assets offered in Hong Kong, we have yet to see any insurer accepting premiums or paying claims in cryptocurrencies or digital tokens in Hong Kong.
INDONESIA	As far as we are aware, insurtech/insurance operations in Indonesia have yet to use cryptocurrency or digital tokens.
JAPAN	Some non-life and life insurance companies started demonstration experiments of issuance and utilization of digital currency the in insurance business since around 2020. However, it seems that utilization of cryptocurrencies or digital tokens are still being studied by insurance companies.
MALAYSIA	No. We are not aware of cryptocurrency or digital tokens being used within insurance operations in Malaysia.
PHILIPPINES	No. While certain fintech companies are now expanding into including cryptocurrencies in their products and services, the Insurance Commission in Circular Letter No. 2020-70, explicitly excluded cryptocurrencies and virtual currencies as digital money for digital payments in insurance transactions.
TAIWAN	No. Neither cryptocurrencies nor digital tokens are used within insurtech/insurance operations.

15 Market Trends

Are cryptocurrencies or digital tokens used within insurtech/insurance operations? (cont'd)

THAILAND	Currently, cryptocurrencies or digital tokens are not used within insurtech/insurance operations.
VIETNAM	No. The SBV prohibits the use of cryptocurrencies as payment instruments.

FOR MORE INFORMATION ABOUT THIS GUIDE, PLEASE CONTACT:

CHINA

Adu Hu
Partner
Tel: +86 10 5649 6080
huguangjian@fenxunlaw.com

HONG KONG

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

INDONESIA

Gerrit Jan Kleute
Foreign Legal Consultant
+62 21 2960 8516
gerrit.kleute@bakermckenzie.com

JAPAN

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

MALAYSIA

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

PHILIPPINES

Dennis Quintero
Partner
Tel: +63 2 819 4962
dennis.quintero@quisumbingtorres.com

SINGAPORE

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

TAIWAN

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

THAILAND

Sivapong Viriyabusaya
Partner
Tel: +66 2666 2824 x4041
sivapong.viriyabusaya@bakermckenzie.com

VIETNAM

Thanh Hai Nguyen
Special Counsel
Tel: +84 24 3936 9606
thanhhai.nguyen@bakermckenzie.com

THE BAKER MCKENZIE
ASIA PACIFIC INSURANCE GROUP

With 17 offices in Asia Pacific, across major cities and emerging markets (including seven of the ASEAN economies), Baker McKenzie has a strong client service platform that few other firms can match in terms of geographical coverage and breadth of practice. Our long experience in Asia Pacific means that we have established experience and interaction with relevant regulators in each jurisdiction. The depth of our legal knowledge in the region is unrivaled as our lawyers combine local industry expertise and understanding, together with international experience. We have worked with many major international and local insurers, insurance intermediaries, and self-regulatory bodies across a spectrum of matters. We fluently apply our extensive industry experience to help develop innovative, compliant and value-driven products.

Our insurance group covers a wide range of services and is frequently cited and consistently ranked among the best in their respective markets. Client-focused and committed to excellence, we observe rigorous service standards to ensure our clients receive consistent and seamless service in Asia Pacific and across the globe.

Through our innovative consulting approach, we give practical and timely advice to help our insurance clients gain a competitive advantage in a highly regulated industry, allowing them to compete confidently across various jurisdictions in the region.

Leading and closing complex deals - every day

We are a transactional powerhouse providing commercially-focused, end to end legal advice to maximize deal certainty and secure the intended value of transactions. Our 2,500 lawyers combine money market sophistication with local market excellence. We lead on major transactions with expertise spanning banking and finance, capital markets, corporate finance, restructuring, funds, M&A, private equity and projects. The combination of deep sector expertise, and our ability to work seamlessly across each of the countries where we operate, means we add unique value in shaping, negotiating and closing the deal.

bakermckenzie.com/transactional