Asia Pacific Insurance - Indonesia

Guide to Insurtech Innovation and Utilization

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Who are the relevant regulators in the region?

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

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

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

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

# What are the types of fintech/insurtech activities that are regulated?

In brief, there is no specific regulation for insurtech activities, which is a relatively new concept in Indonesia.

Although there are no specific fintech/insurtech regulations, the government is aware of technological developments and is now encouraging fintech/insurtech activities. Current laws and regulations impacting on fintech/insurtech activities include the following:

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

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

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

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

Bank Indonesia Circular Letter No. 16/11/DKSP, dated 22 July 2014 as amended by Bank Indonesia Circular Letter No. 18/21/DKSP dated 27 September 2016 on the Implementation of E-money Operations, regulates electronic money.

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

Although there are no specific fintech/insurtech regulations, the government is aware of technological developments and is now encouraging fintech/insurtech activities and has acknowledged that a regulatory framework needs to be put in place.

# What are the licenses required and what are the criteria and process involved?

The licenses required will depend on the specific activities contemplated:

Insurance. In the absence of a specific regulation on insurtech, no specific license is required if an insurance company sells an e-policy.

Insurance broker. Am insurance broker business must obtain a business license from the OJK (whether services are offered through digital channels or not).

E-money. Licenses for e-money activities must be obtained from Bank Indonesia.

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

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

Remittance business. Licenses for remittance activities must be obtained from Bank Indonesia.

Crowdfunding: Public crowdfunding activities require an effective statement from the OJK.

Intellectual property registrations. For completeness, if the fintech/insurtech innovation involves a patentable invention or if there are plans to register a trademark, investors need to register matters.

# Is the use of telematics and/or biometrics regulated?

There is no regulation regarding telematics and biometrics in Indonesia. The utilization of telematics and biometrics in Indonesia itself is still relatively rare.

In relation to personal data used in biometrics, under MOCI regulation the use, broadly defined, of any data analytic activities using customers' personal data must have received a specific consent from the data owner/customer.

# Does the regulator draw a distinction between institutions that are "too big to fail" versus "too small to care"?

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

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

There are no specific laws and regulations in the insurance sector prescribing rules on technology risk management. The existing regulations are more general in nature, old school and are principle-based regulations (rather than regulations that clearly set out relevant
requirements). Given the absence of clear requirements, businesses need to be prudent, take security steps, do due diligence and ensure that internal control systems are properly implemented.

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

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

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

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

maintain the confidentiality, unity and availability of private data

secure that the collection, use and utilization of private data is done upon the consent of the owner of private data, unless provided otherwise by applicable laws and regulations

secure that the use or disclosure of data is conducted with the consent of the owner of private data and in accordance with the purpose conveyed to him/her at the time of collection of the private data.

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

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

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

POJK 1 provides that consent from customers on the use of their data (including to transfer the data) must be obtained in writing.

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

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

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

Data and information related to the personal data of the policyholder, the insured, or participants (name, address, date of birth, etc.)

Data and information relating to premium payments or claims

Data and information on the nationality (national ID number or passport details)

Data and information on the relevant legal entities (tax file number of participants, business license registration number, etc.)

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

No. However there is an express requirement to obtain written specific consent from customers before transferring data. Businesses need to consider the most practical way to obtain the written consent from customers. In practice, insurance companies include the consent
in their standard insurance policy clause. Given the Data Protection Regulation (fully effective in December 2018), insurance companies must refine their consent language to conform with the Data Protection Regulation. Before the Data Protection Regulation was enacted, consent language could be very broad and general (for example, a blanket approval). Now consents must be very specific. For example, the customer must know and specifically consent to the actual use of that data (such as data analytics).

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

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

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

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

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

We are not aware of any fintech/insurtech cases (noting that there are no law reports in Indonesia).

# What are the most immediate challenges to insurtech innovation?

Regulations – The government acknowledges that it is likely to be behind market developments in regulating fintech/insurtech activities. Consequently there is less clarity for businesses as to how matters may be regulated, and reliance on older regulations,
which may not be as conducive to the fintech/insurtech sector (for example, written consent for data use and transfer). In November 2016, Bank Indonesia established a dedicated fintech office within its organization to assist fintech start-ups in risk assessment, licensing coordination and a regulatory sandbox. The effectiveness of this fintech office remains to be seen.

Technology – Local technology may not be sufficient to accommodate the development of fintech products.

Customers – Although internet utilization is becoming more common in Indonesia and Indonesians are more tech-savvy than before, customers may take time to accept fintech/insurtech. Currently most selling of financial products is personal in nature (for example, telemarketing and agents). Customers will need more assurance and more time to accept fintech/insurtech services.

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

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

# What insurtech trends or disruptions may impact insurance companies?

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

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

©Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction**: Reproduction or copying of the Content on this Site without express written authorization is strictly prohibited.