Asia Pacific Insurance - Philippines

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 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.

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

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

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

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

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

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

Based on our experience, regulators are generally receptive to the introduction in the Philippines of fintech products and services that have been introduced in many other countries, subject to the regulator's imposition of certain conditions for the protection of the public. Regulators view fintech as a way of pursuing financial inclusion through digital technology. Having said that, the process of getting such regulatory confirmation/approval of a fintech product or service that is not specifically governed by existing laws and regulation usually takes time, and the grant of confirmation/approval is subject to the regulator's sole discretion.

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

The IPOPHL fully supports technological innovation, including financial technologies. To this end, the IPOPHL has established a nationwide network of Innovation and Technology Support Offices, which assists local innovators in claiming and protecting their intellectual property rights.

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

Entities engaged in fintech products/services relating to e-money and remittance services (including virtual currency exchange systems), are generally required to obtain a license or authority from the BSP.

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

For the following activities, a financial services 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.

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

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

For patents, information is available at <http://info.ipophil.gov.ph/dev/services/patents/patent-application-flow-chart>
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>

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

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).

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

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

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

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

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

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

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.

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

Insurance companies should comply with the Guidelines on Electronic Commerce of Insurance Products issued by the Insurance Commissioner. The guidelines provide for online privacy requirements and security of payment and personal information, among others.

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

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

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

Sensitive personal information, which refers to personal information: (a) about an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (b) about an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (c) issued by government agencies peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (d) specifically established by an executive order or an act of Congress to be kept classified.

The principal requirement under the DPA for the processing of personal data is the consent of the data subject. As a general rule, the consent of the data subject to the processing of his or her personal data is required, and must be evidenced by written, electronic or recorded means. If personal data is intended to be shared or transferred to third parties, service providers or other data processors, the data subject’s specific consent to such data sharing would also be required. The timing of the consent would vary depending on the type of information involved in the processing. If the information pertains to simply personal information, then consent must be procured prior to the collection, or as soon as practicable and reasonable. On the other hand, with respect to the processing of sensitive personal information, the DPA exacts a stricter standard: the data subject’s consent at all times must be procured prior to the processing of the
sensitive personal information.

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

Yes. The DPA imposes stringent compliance obligations on persons or entities engaged in the processing of personal data.

For instance, under the DPA, personal information controllers and processors shall have the following responsibilities:

ensure that proper safeguards are in place to guarantee the confidentiality of the personal information processed and prevent its use for unauthorized purposes

implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing

use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party

designate an individual, called a data protection officer, who is accountable for the entity's compliance with the DPA

Furthermore, the DPA mandates the registration of processing systems of personal information controllers and processors that are involved in the processing of sensitive personal information of at least 1,000 individuals, whether it be of employees, clients, customers or contractors. The current deadline for this registration requirement is on 9 September 2017. Note that failure to comply with the DPA may mean not only mandatory business closure for the controller and processor but also payment of damages and of steep fines. For responsible officers and employees, non-compliance by their organizations may even result to imprisonment.

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.

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

The Cybercrime Law enumerates and punishes cybercrimes, imposes duties upon service providers, and provides tools for enforcement of cybersecurity.

Under the Cybercrime Law, a service provider is an entity that provides users of its service with the ability to communicate by means of a computer system. It can also be an entity that processes or stores computer data on behalf of such communication service or users of
such service.

A service provider is expected to do the following:

disclose or submit subscriber's information, traffic data or relevant data in its possession or control to competent authorities within 72 hours after the receipt of an order to submit

collect or record by technical or electronic means, and/or cooperate and assist competent authorities in the collection or recording of computer data upon the issuance of a court warrant

report to the OCC its compliance with enforcement orders and reporting requirements under the Cybercrime Law

immediately and completely destroy computer data subject of a preservation and examination when the required period expires

ensure the confidentiality of preservation orders issued

The Cybercrime Law also enumerates cybercrimes, including computer-related forgery, computer-related fraud and computer-related identity theft. It also punishes certain offenses that violate the confidentiality, integrity and availability of computer data and systems. Among such crimes are illegal access to computer systems, illegal interception of computer data, unauthorized data interference, unauthorized system interference, misuse of devices and cybersquatting.

Similarly, the DPA also punishes the unauthorized access or intentional breach of any system where personal data is stored.

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

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

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

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.

# What are the most immediate challenges to insurtech innovation?

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.

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

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.

# What insurtech trends or disruptions may impact insurance companies?

We expect insurance companies partnering with insurtech and technology entities to help them develop their technology and business strategies.

©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.