Asia Pacific Insurance - Australia

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

# Guide to Insurtech Innovation and Utilization

## Who are the relevant regulators in the region?

The Australian Securities and Investments Commission's (**ASIC**) and the Australian Prudential Regulation Authority (**APRA**) are the two main regulators for the fintech/insurtech industry.

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

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

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

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

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

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

Companies seeking to provide any financial or insurance products or services are required to hold an Australian Financial Services Licence (AFSL) or a credit license. However, ASIC's regulatory sandbox allows eligible fintech/insurtech businesses to:

test certain financial and credit services for up to 12 months without needing to apply for a financial services or credit license

offer products and services to wholesale clients and a limited number of retail clients (up to 100 retail clients only), with appropriate monetary exposure limits in place

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

dealing in all listed or quoted Australian securities

all deposit products

debentures, stocks or bonds issued or proposed to be issued by the Australian government

simple managed investment schemes (that is, a registered scheme that invests at least 80% of its assets in a bank account where funds can be withdrawn within three months, or in arrangements where the investments can be realized at market value within 10 days)

home contents insurance products

personal and domestic insurance products

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

extend the testing time frame to 24 months

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

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

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

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

home contents insurance products (for example, household goods and jewelry)

personal and domestic insurance products (for example, mobile phone insurance)

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

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

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

The licenses required will depend on the specific activities contemplated. The key licensing and/or regulatory requirements include:

Financial services or credit licenses – Businesses conducting a financial services business or providing credit require the relevant financial services or credit licensing conditions from ASIC.

ASIC regulatory sandbox exemption – Businesses that qualify under ASIC's regulatory sandbox may apply to ASIC to have their licensing requirements waived. As discussed (at question 2), eligible start-ups that qualify to operate under ASIC's regulatory sandbox  
may operate for 12 months without needing to apply for a financial services or credit license, provided that products and services are offered to wholesale clients and a limited number of retail clients (up to 100 retail clients only), with appropriate monetary exposure limits in place. ASIC may further use its waiver (relief) powers on a case-by-case basis.

Authorized deposit-taking institution (ADI) – Institution seeking to be regulated as an ADI will require the relevant licenses with APRA.

Equity crowdfunding – Companies looking to facilitate capital raising under the Australian government's latest crowdsourced equity funding framework starting in September 2017 will require a financial services license. Among other things, this allows eligible companies to raise up to AUD 5 million per year if they have less than AUD 25 million in gross asset value.

Venture capital – Fintech/insurtech investors may apply to Innovation Australia to be structured as a venture capital limited partnership (VCLP), or early-stage venture capital limited partnerships (ESVCLP) under the Venture Capital Act 2002 (Cth) and receive  
more favorable tax treatment for investment.

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

There are no specific regulations for the use of biometrics on its own. Biometric data is regulated by the Privacy Act 1988 (Cth). The Australian Law Reform Commission (ALRC) has also recently recommended that certain biometric information be labelled as sensitive information to afford consumers greater protection.

The Intelligent Access Program (IAP), is a national program developed in partnership with all Australian road agencies, and is the first road regulatory use of telematics in Australia. The IAP relies on certified telematics providers (IAP service providers) and their approved GPSbased  
telematics devices and systems (approved intelligent transport systems) to offer road authorities a compliance solution when it comes to allowing operators of certain vehicles access or enhanced access to the public road network.

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

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

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

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

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

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

From a personal data privacy perspective, insurance companies must take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information. An insurance company that holds personal  
information must:

take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorized access, modification or disclosure

take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs

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

The Privacy Act 1998 (Cth) governs the collection, use, storage, disclosure and transfer of personal data. The Privacy Act applies to companies with an annual turnover of more than AUD 3 million (APP entity).

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

Open and transparent management of personal information – All entities subject to the Privacy Act must have an APP Privacy Policy.

Anonymity and pseudonymity – Individuals should have an option of not identifying themselves when dealing with an organization, unless this is impracticable or the organization is required by law to deal with an individual on an identified basis.

Collection of solicited personal information – An organization must not collect personal information unless reasonably necessary for one or more of the entity's functions or activities.

Dealing with unsolicited information – An organization must take specific steps if it obtains personal information that it did not specifically solicit.

Notification – Individuals must be provided with a collection statement before or at the time their information is collected.

Disclosure for a primary purpose – Use or disclosure of personal information is not permitted for purposes other than the primary purpose for which it was collected.

Direct marketing – Subject to exceptions, use or disclosure of personal information for direct marketing purposes is not permitted without consent.

Cross-border disclosure of personal information – Entities are required to take reasonable steps to ensure that an overseas recipient of Australian personal information does not breach the APPs, and such entity will remain liable for any misuse by the overseas  
recipient.

Integrity of personal information – An organization may not adopt a government-related identifier (such as a tax file number) as its own identifier.

Quality of personal information – An organization must take reasonable steps to ensure that personal information it collects, uses or discloses is accurate, up to date and complete.

Security of personal information – An organization must take reasonable steps to protect personal information it holds from misuse, interference and loss as well as from unauthorized access, modification or disclosure.

Access to personal information – Individuals have a right to access their personal information on request.

Correction of personal information – Organizations must take reasonable steps to correct personal information on request by an individual.

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

To the extent that the insurance company has an annual turnover of more than AUD 3 million per year, its activities and usage of insurtech remains subject to the Privacy Act and the requirements of the APPs as set out in response to question 3(a) above.

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

The Privacy Act governs the security obligations relating to personal information.

Cybercrime Act 2001 criminalizes various computer activities such as hacking, virus propagation, denial of service attacks, and website vandalism.

Australian Security Intelligence Organisation (ASIO) Act 1979 governs the conduct of Australia's counter-intelligence and security agency and sets out various investigative powers available to ASIO under warrant, including in relation to suspected cybercrime.

Telecommunications Act 1997 and Telecommunications (Interception & Access) Act 1979 also permits access to communications content held by carriage service providers and licensed telecommunications carriers for law enforcement and national security purposes under warrant.

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

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

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

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

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

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

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

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

There have been no specific cases in relation to fintech/insurtech cases to date.A

## What are the most immediate challenges to insurtech innovation?

The high costs of development and innovation – While there is high demand from insurers looking for new technologies to improve customer service and transform operational models, there are still many insurance companies that do not have a budget allocated for innovation, or someone actually responsible for innovation. See KPMG's insurtech research at: https://home.kpmg.com/au/en/home/  
insights/2017/03/insurtech-dilemma-insurance-technology.html.

Regulation – High levels of regulation from ASIC and APRA present a significant barrier to entry. Industry groups are seeking support form the Australian government for increased flexibility to support emerging micro-insurance and quasi-insurance models (for  
example, self‑funded excess and peer‑to‑peer insurance), which are not readily facilitated by current models. See https://fintech.treasury.gov.au/australias-fintech-priorities/

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

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

## What insurtech trends or disruptions may impact insurance companies?

We can expect to see a rise in insurance companies acquiring or teaming up with tech-focused companies (including digital insurance start-ups or telematics-related companies) in order to deliver new products and better price risk. The three main trends or disruptions include:

Increase in collaboration between start-ups and incumbents: high barriers to entry to the insurance industry could restrict a wave of new stand-alone e-insurance brokers, which would need to work with traditional insurance companies.

Insurance telematics: with insurance telematics, insurers can have better information and can expect a rise in usage-based insurance and dynamically adjusted premiums, moving away from conventional static premiums. Further, insurance telematics can help improve risk management, drive cost down for claims process, enhance customer loyalty through creating opportunities for regular contact and potentially open up new possibilities for sales channels and revenue-generating services in partnership with businesses from other sectors.

Improved data analytics: With improved data analytics, the old-fashioned actuarial tables of insurance companies can be enhanced with real-time data and dynamic pricing. Wearable tech and telematics also give companies more personalized data.

# Guide for Insurance Sales, Advisory and Distribution

## What are the different types of insurance intermediaries in the market and do they need to hold any licenses and minimum qualification to conduct business?

In Australia, a person commits an offense if the person carries on an insurance business and is not a general insurer authorized to do business in Australia by the Regulator (the Australian Prudential Regulation Authority or APRA). This also applies to foreign general insurers. Intermediaries of authorized general insurers are any persons, including agents and brokers, who provide financial product advice or deal in insurance contracts. They must obtain an Australian Financial Services License (AFSL) unless they do so as a representative of an existing license holder, or fall within certain exceptions. Several requirements must be satisfied for the grant of an AFSL. These requirements include training of representatives, adequacy of dispute resolution systems, systems for the management of conflicts of interest, and adequate resources including financial, technological and human, which relate to risk management. If a person is to conduct business as a representative of an AFSL holder that is an authorized general insurer, that person must hold an approved formal qualification, meet statutory work experience standards, be "fit and proper" and demonstrate approved evidence of ethical compliance.

## Is it mandatory for insurers to offer customers the option of purchasing insurance products directly from them without going through financial advisers or intermediaries?

No. Certain types of products may be purchased directly from insurers and others are more commonly purchased through intermediaries. It is not mandatory to offer insurance directly to customers first. Whether an insurer can offer products directly depends on the terms of the insurer's AFSL. Most general insurers in Australia sell retail insurance via a "no advice or general advice" model and will not be licensed to advise customers on insurance products. Typically, an intermediary will advise customers and will have product advice allowances under its own AFSL (or under that of the person of whom it is an authorized representative). Intermediaries have obligations if they are providing personal or general advice to customers. They must issue Financial Services Guides that contain warnings to protect the customer and disclosure of commission if the service is typified as "personal" under the Corporations Act 2001 (Cth).

## Do agreements between insurers and their agents need to take a certain form?

No. There is no restriction on the format of such agreements. Any written authorization by an AFSL holder in favor of a third party to be its representative can only carry with it such rights as are conferred upon the AFSL holder under the terms of its license. All such authorizations must also be notified to ASIC within 30 business days.

## Can insurers pay volume-based commission to their appointed agents?

Generally, no. Volume-based commission is assumed to be "Conflicted Remuneration" under the Corporations Act 2001 (Cth). It is an offense under section 963 of the Corporations Act 2001 to facilitate it or collect it. There are some exceptions, such as where the commission (or benefit) is given to the AFS License holder or broker solely in relation to a general insurance or life risk product.

## Are insurers liable for any mis-selling of its agents or appointed distributors?

Yes. Under Chapter 7 of the Corporations Act 2001, there is a general liability of AFSL holders for the acts of their agents. In addition, the Act contains more specific provisions that impose strict liability upon an AFSL holder (sections 917B and 917C) for the acts and omissions of its authorized representatives. The quantum of liability is for any loss or damage suffered by the customer (section 917E).

## Are there rules on the number of insurers that insurance brokers need to present to their customers?

No. However, there is a common law duty of care not exempted by the Act that requires an agent to act in the best interests of its client. In addition, under sub sections G, H and J of the Corporations Act, which apply to authorized representatives, the authorized representatives must provide appropriate advice to the customer that must not be based on incomplete information. Further, under section 961J, where there is a conflict of interest, the authorized representative must give priority to the customer's interests when giving the advice. There is an exception where the subject matter is in relation to a general insurance product. It is possible to be the authorized representative of more than one AFS License holder (section 916C of the Corporations Act 2001), though this can only occur if each AFSL holder consents to the other, and to the authorization of the common representative. If there are two AFSL holders, one can be appointed as the authorized representative of the other but only where one is an insurer and there is a "binder" given by the insurer.

## Can insurance brokers receive commission from both insurers and their customers? If so, can they be volume-based commission?

There is no statutory prevention from receiving commission generally from both insurers and the customer. Volume-based commission is illegal unless it is in relation to a general insurance or life risk product (section 963 of the Act). Where commission is received from both customer and insurer, the party in whose interests the broker is acting particularly may also lead to conflict of interest, which is also a breach of the Corporations Act 2001. In addition, the Corporations Act 2001 requires brokers who provide general or personal financial advice to issue a "Financial Services Guide" to the customer. Where the advice is considered personal to the customer, then all  
remuneration and commission must be fully disclosed in advance of the service being provided.

## Can agents or appointed distributors offer rebates on insurance premiums or other special concessions to the customers?

Subject to the following, there is no specific legislative prevention. However, in relation to general and other insurance, there are statutory circumstances which govern the cancellation and termination rights of an insurer and which are not capable of being modified or limited by contract. Examples are contained in the Insurance Contracts Act 1984 (Cth). How much premium was rebated would depend on that which is yet to be earned at the time of cancellation or termination and the provisions of the policy. Otherwise, the offering of concessions or rebates to attract customers is likely to attract the adverse attention of both ASIC and APRA (the regulators). For example, it is an offense under section 1041 of the Corporations Act 2001 to create an artificial price or market for the trading of financial products.

## Can insurers appoint offshore agents or accept business from offshore brokers?

Generally, no. If offshore business is to be carried on in Australia, it must be through a registered general insurer who has an Australian Financial Services License. That insurer may accept business under the terms of its Australian Financial Services License. However, if the offshore agent or broker is "carrying on a financial service business" in Australia as defined by Division 4 of Part 7.1 of the Corporations Act, it will likewise require an AFSL to place that business in Australia. If the agent or broker is providing financial product advice (section 766B), or is dealing in a financial product (section 766C), or is making a market for a financial product (section 766D), it may be carrying on such a business. To do so without an AFSL is an offense under section 911A.

## Are there specific requirements on selling products through call centers, telemarketing or other distribution channels?

Yes. There are requirements and restrictions under the Corporations Act 2001 relating to where a financial service is being provided by brokers and intermediaries notwithstanding whether through call centers, telemarketing or other distribution channels. A product disclosure statement must be in writing and be issued to the customer at the point of sale (under Division 2 of Part 7.9 of the Corporations Act 2001). Prior to provision of the service, the provider of a "Financial Service" should also issue a Financial Services Guide to the customer. Whether a distributor is providing a financial service under the Act will depend on the circumstances. There are  
requirements concerning the handling of money, the confirmation of transactions (section 101), requirements for marketing (Division 5) and cooling-off periods (Division 5). A regulatory guide issued by ASIC explains the approach to compliance and enforcement (ASIC Regulatory Guide 168). There are a number of specific offenses for non compliance.

## Are there specific requirements on selling products through online channels?

Yes. The Corporations Act 2001 and its regulations contain specific requirements concerning the sale of products online. The usual Corporations Act 2001 requirements concerning product disclosure and financial services guides still apply. Full product disclosure must still be made of the product, at or before sale (section 1012C). If the product is issued online, product disclosure must be provided in electronic form (Reg 7.7.01). Timing is important. In addition and in relation to data security, APRA has issued Prudential Practice Guide "CPG 234 Management of Security Risk in Information and Information Technology," which details the measures it expects to be taken  
by insurers to minimize online and technology risk. Examples of these protections include encryption and the use of keys or triple block ciphers (algorithms) to protect authenticity of information and prevent the unauthorized alteration of data. Customers who buy products using electronic payment facilities are protected by the "ePayments Code," which is regulated by ASIC.

## Can insurers share client information with insurance agents and brokers and vice versa? What data privacy or confidentiality laws apply?

The Australian Privacy Act 1988 (Cth) regulates how insurers can share client personal information such as an individual's name, date of birth, address, phone number, etc., with third parties such as insurance agents and brokers and vice versa. Under Australian Privacy Principle (APP) 5, an entity is required to take reasonable steps to notify an individual of certain collection-related information at, before, or if not practicable, as soon as practicable after the time of the collection, including information about any entities to whom that entity usually discloses personal information of the kind collected (in this case, insurers, insurance agents or brokers, as relevant), as well as make available a privacy policy.

Any disclosures to third parties who are not specified in the original collection statement or privacy policy can be made only with the individual's consent unless certain exceptions apply including if disclosure is for a purpose related to the primary purpose of collection and the individual would reasonably expect such disclosure, or where the use or disclosure is required or authorized by an Australian law or court/tribunal order.

For disclosures outside of Australia, reasonable steps must be taken to ensure the overseas recipient does not breach the APPs. The disclosing entity will be strictly liable for any such breach unless certain exceptions apply, including where consent is obtained or where the overseas recipient is subject to a law or binding scheme that has the effect of protecting the information to at least a substantially similar level to the Privacy Act and the individual would have recourse under the relevant law or scheme.

# Investing in Insurtech Start-ups

## Are there any limitations or criteria on the type of start-up that an insurer can invest in? Does the start-up need to be registered with any authority?

Subject to an insurer meeting its ongoing Australian prudential obligations and controls (as stipulated by Australian Prudential Regulation Authority or APRA), there is no "per se" restriction on an insurer investing in a start-up organization.

## What are the available options in terms of investments that an insurer can make in an insurtech start-up?

The insurer can invest in an insurtech start-up either as equity instruments or by granting of loans.

## What are the restrictions on investing in an onshore insurtech start-up?

Subject to an insurer meeting, its ongoing Australian prudential obligations and controls (as stipulated by APRA), there is no "per se" restriction on an insurer investing in an on-shore start-up.

The Commonwealth Insurance Acquisitions and Takeovers Act 1991 regulates acquisitions and takeovers of general and life insurance companies. Its aim is to protect the public interest. In particular, it regulates the parties allowed to take control of insurance companies, and regulates the concentration of economic power in the insurance industry or financial system. The relevant minister considers takeover proposals and may make a temporary or permanent restraining order, or a divestment order.

## What are the restrictions on investing in an offshore insurtech start-up? Is approval required from the regulators?

Subject to an insurer meeting its ongoing Australian prudential obligations and controls (as stipulated by APRA), there is no "per se" restriction on an insurer investing in an offshore start-up.

## Is an insurer permitted to grant loans to an insurtech start-up? Under what conditions?

The provision of a loan is heavily regulated in Australia. We note the following in relation to granting a loan:

Banking legislation – Provided the insurer is not also taking any money on deposit, then it is unlikely that granting a loan to an insurtech start-up will be subject to this legislation. However, we note that carrying on a banking business in Australia (which consists of taking deposits and making advances) requires registration as an Authorized Deposit-Taking Institution (ADI) under the Banking Act 1951 (Cth) ("**Banking Act**") or an exemption from the requirement to be registered as an ADI. Any insurer contemplating the granting of a loan should consider this regulation.

National Credit Code – Provided the loan is not granted to a natural person or strata corporation and is not wholly or predominantly for personal, household or domestic purposes, or residential property investment, then it is unlikely that granting a loan to an insurtech start-up will be subject to this legislation. However, we note that a person who engages in credit activities to which the National Credit Code applies (for example, providing a loan to a natural person or strata corporation, that is provided wholly or predominantly for personal, household or domestic purposes, or residential property investment) requires an Australian credit license (ACL). Any insurer contemplating the granting of a loan should consider this regulation.

AML/CTF – Under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) ("**AML/CTF Act**"), providing a loan is a regulated service and will require the provider of the loan to register with the Australian Transaction Reports and Analysis Centre and comply with the obligations under the AML/CTF Act (for example, customer due diligence, having a compliance program in place and reporting certain things to the regulator). In some circumstances, it is appropriate to apply to the regulator for bespoke relief from the registration requirements. This is determined on a case-by-case basis. Any insurer contemplating the granting of a loan should consider this regulation.

## What type of corporate approvals is required for an insurer to invest in an insurtech start-up?

If the insurer is publicly listed in Australia, then usually it would simply require the consent of the board of directors. Given the relatively small size of start-ups, an investment in one would be very unlikely to trigger a requirement for shareholder approval under the relevant listing rules.

## Are there any general minority shareholder protection mechanisms in your jurisdiction?

Section 232 of the Corporations Act 2001 (Cth) provides protection to a shareholder who has been oppressed, or treated in an unfairly prejudicial way or unfairly discriminatory way.

## Are there any restrictions on the insurer in terms of appointing its own staff or management to join the insurtech start-up's board of directors or management team?

There are no restrictions on the insurer as regards appointing its staff or management to join the insurtech start-up's board of directors or management team.

## Are there any restrictions on entering into a service contract with the insurtech start-up upon completion of the investment? (a) Any connected party transaction restrictions? (b) Any prerequisite approvals required from the regulators or from internal committees?

There are none.

There are standard internal governance controls for making any asset investment by an insurer (for example, relevant investment committee, risk committee). In terms of regulatory controls, please see question 3.

## Are there any regulatory requirements on the disclosure of the transactions and connected transactions thereafter between the insurer and the insurtech start-up?

Financial services: There are no specific requirements to disclose transactions between the insurer and the insurtech start-up. That being said, where permitted by law, such disclosure may be required in order to satisfy Australian financial services license conditions (the insurer and insurtech company will likely hold this license). This will depend on the exact licensing arrangements of each party.

AML/CTF: There are transaction reporting requirements imposed on entities that provide certain life insurance products. These transaction reporting requirements oblige the regulated entities to report transactions to the regulator and not to each other. Some customer due diligence outsourcing arrangements will require the parties to share/disclose transactions to each other.

## To what extent can the insurer provide operational support to the insurtech start-up?

Financial services: If operational support constitutes the provision of a "financial service" for the purposes of the Corporations Act, then the insurer can only provide such support if it is appropriately licensed or exempt from the licensing requirement. The operational support services will constitute a financial service if:

the provision of financial product advice is involved (a person provides financial product advice if they provide a recommendation, statement of opinion or report on either of those things that is intended to influence a person or persons in making a decision in relation to insurance products or could reasonably be regarded as being intended to have that influence)

dealing in an insurance product is involved (a person deals in a financial service if they issue an insurance product, vary an insurance product, dispose of an insurance product arrange for another person to do any of the above things in respect to an insurance product)

If no "financial services" are involved in the operational support services, then the insurer can provide those services.

## What type of remuneration is permitted for the insurer to offer to the insurtech start-up?

Financial services: Please note that there are conflicted remuneration provisions under the Corporations Act that ban commission-type or volume-based payments (with some exceptions). There is an exemption for general insurance products; however, insurers would need to ensure that the particular insurance product they wish to remunerate in relation to falls within that exemption.

## How can the insurtech start-up transfer the intellectual property rights for its

Insurtech companies can transfer or grant licenses to use intellectual property rights through agreements describing and implementing such arrangements. Registered intellectual property rights like patents, trademarks and registered designs will need to have their registration details updated in order to reflect any transfer of ownership, as these registers are the primary evidence of rightsholders' identities in such intellectual property.

## Are there any laws governing the collection, usage, storage, disclosure and transfer of personal data between the insurer and the insurtech start-up?

The Commonwealth Privacy Act 1988 regulates the way personal information is collected and handled by both government and private organizations. Regulated organizations must handle personal information in accordance with the 13 Australian Privacy Principles set out in that act. There are also state-based regulations relating to information privacy, particularly relating to government agencies collecting, managing and disclosing personal information.

# Data Protection and Cybersecurity

## Who is the main regulator with oversight of data privacy matters?

The Office of the Australian Information Commissioner (OAIC)

## What is the main legislation on the protection of personal data privacy?

Privacy Act 1988 (Cth)

## Who is the main regulator with oversight of cybersecurity matters?

There is no particular regulator tasked with oversight of cybersecurity matters per se. The OAIC is the relevant regulator if personal data is involved. The Australian Prudential Regulatory Authority (APRA), the regulator which oversees banks, other financial institutions and insurance industries, provides a set of standards/guidelines in relation to IT security, which applies, among other institutions, to general insurance, life insurance and superannuation industries. The Australian Securities and Investments Commission (ASIC) also may have some oversight of cybersecurity matters in the insurance industry.

## Is there existing legislation governing cybersecurity issues?

The Privacy Act, which governs personal information; the Cybercrime Act 2001; Australian Security Intelligence Organisation (ASIO) Act 1979; Telecommunications (Interception & Access) Act 1979; Telecommunications Act 1997; Spam Act 2003.

## What are the main requirements with respect to collection, use, disclosure or transfer of personal data?

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

Open and transparent management of personal information – All entities subject to the Privacy Act must have an APP Privacy Policy.

Anonymity and pseudonymity – Individuals should have an option of not identifying themselves when dealing with an organization, unless this is impracticable or the organization is required by law to deal with an individual on an identified basis.

Collection of solicited personal information – An organization must not collect personal information unless reasonably necessary for one or more of the entity's functions or activities.

Dealing with unsolicited information – Organization must take specific steps if it obtains personal information that it did not specifically solicit.

Notification – Individuals must be provided with a collection statement before or at the time their information is collected.

Disclosure for a primary purpose – Use or disclosure of personal information is not permitted for purposes other than the primary purpose for which it was collected.

Direct marketing – Subject to exceptions, use or disclosure of personal information for direct marketing purposes is not permitted without consent.

Cross-border disclosure of personal information – Entities are required to take reasonable steps to ensure that an overseas recipient of Australian personal information does not breach the APPs, and such entity will remain liable for any misuse by the overseas recipient.

Integrity of personal information – An organization may not adopt a government-related identifier (such as a tax file number) as its own identifier.

Quality of personal information – An organization must take reasonable steps to ensure that personal information it collects, uses or discloses is accurate, up to date and complete.

Security of personal information – An organization must take reasonable steps to protect personal information it holds from misuse, interference and loss as well as from unauthorized access, modification or disclosure.

Access to personal information – Individuals have a right to access their personal information on request.

Correction of personal information – Organizations must take reasonable steps to correct personal information on request by an individual.

## What are the main requirements for ensuring security of personal data?

Under APP 11, an APP entity must take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information. An APP entity that holds personal information must do the following:

take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorized access, modification or disclosure

take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs

## Are there additional requirements with respect to "sensitive personal data"?

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

the entity obtains the consent of the individual and the information is reasonable necessary for the activities or functions of the entity

collection is required by law

collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where it is unreasonable or impracticable to obtain the consent of the individual to whom the information relates

the information is collected by a nonprofit organization and relates solely to the organization’s activities and to the organization’s members or persons who have regular contact with the organization in connection with its activities

collection is necessary for the establishment, exercise or defense of a legal or equitable claim

where the entity is a Commonwealth enforcement body, the collection is necessary for the performance of that enforcement body’s functions or activities

the information is collected in the process of providing a health service, and is either collected as authorized by law or subject to a professional code of ethics

the information is collected in the course of medical research that is subject to professional safeguards and where obtaining consent is impracticable, and the research cannot be performed without the information being collected

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

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

## Are there additional obligations imposed on insurance companies with respect to collection, use and transfer of personal data of customers? Are there registration requirements to be complied with?

lnsurance companies that are APP entities must comply with their obligations under the Privacy Act as set out in response to questions 5 to 7 above. There are no particular registration requirements to be complied with.

## Are insurance companies required to have a data protection officer?

In Australia, although it is considered best practice to do so, there is no legal requirement to appoint or designate a data privacy officer. However, organizations are required to make available a privacy policy on request from a data subject.

## Do insurance companies need to undertake privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data?

While not a strict legal requirement, APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and enable them to deal with enquiries or complaints about privacy compliance. In this way, the APPs require “privacy by design,” an approach whereby privacy compliance is designed into projects dealing with personal information right from the start, rather than being bolted on afterward. Conducting privacy impact assessments (PIAs) helps entities to ensure privacy compliance and identify better practice. OAIC guidelines recommend and provide guidance for conducting PIAs for “projects” such as the implementation of new or amended programs, activities, systems or databases. Similarly, conducting PIAs would assist in complying with APRA standards surrounding cybersecurity and managing data risk.

## What are data subjects' rights, if any, in relation to the processing of their personal data?`

Data subjects have the general right to:

be informed by an organization of the personal data the organization holds about the data subject

access the data subject’s personal data, subject to some restrictions and/or qualifications

request the correction of the data subject’s personal data

request the deletion and/or destruction of the data subject’s personal data

## Are there restrictions regarding cross-border transfer of personal data for insurance companies?

If an insurance company discloses personal data to a recipient outside of Australia, it must take reasonable steps to ensure that the offshore recipient (including a related entity) does not breach the APPs. Unless an exception applies, if the recipient handles the personal data in a manner that would breach the APPs if that recipient were subject to the APPs, the organization that disclosed the information will be taken to have breached the APPs.

A key exception is if the recipient to which personal data is disclosed is subject to a law or binding scheme which provides the same protection as under the Privacy Act, and there are mechanisms that the data subject can access to enforce that law or binding scheme. A further exception is if the organization expressly informs data subjects that if information is disclosed outside of Australia, the  
organization will not be responsible for any failure of the recipient to protect the personal data in a manner consistent with the APPs, and having been so informed, the data subject consents to the disclosure.

## Are there specific requirements for insurance companies in relation to the use and transfer of personal data for marketing purposes? Can customers opt out?

Whether businesses can use personal data for direct marketing will depend on how they collected the information (whether it was directly from the relevant data subject or from a third party) and whether individuals would reasonably expect their information to be used for this purpose). There is also an opt-out requirement that applies to all direct marketing communications. Additional restrictions apply to the use of Sensitive Data for direct marketing.

In addition to requirements under the Privacy Act, direct marketing communications are also subject to requirements under the Spam Act 2003, which prohibits the sending of electronic commercial messages without consent and require all such messages to contain certain  
information and an unsubscribe facility. The Do Not Call Register Act 2006 prohibits businesses from contacting individuals on the Do Not Call Register by telephone or fax except in certain restricted circumstances.

To the extent the Spam Act or the Do Not Call Register Act applies, the Privacy Act does not apply.

## Are there specific requirements for insurance companies in relation to the receipt of personal data from its business partners?

Where personal data other than sensitive data is collected from a third party, an insurance company may use that data for direct marketing purposes provided that it has (a) obtained the relevant individual's consent for use of its personal data for those purposes; and (b) provided the individuals with a simple way to opt out of receiving direct marketing communications from the organization.

## Can insurance companies transfer the personal data of their insurance agents or intermediaries to other service providers such as investigation agents or debt collectors?

Insurance companies may disclose personal data of their agents or intermediaries to other service providers if such transfer is the primary purpose for collection, or such transfer is a related secondary purpose and an individual may reasonably expect the insurance company to  
disclose their personal information to such third parties. It is advisable for insurance companies to make such uses of personal data clear in their privacy policies and collection notices. If an individual may not reasonably expect the transfer of their personal data in this way, then their consent must be obtained before doing so.

## Are there additional regulatory requirements imposed with respect to the outsourcing of data processing to third-party data processors?

Organizations that disclose personal data to third parties should ensure there are contractual or other means in place to protect the personal data. In case of a data breach incident, the outsourcing organization may be held liable together with the third-party provider.

When outsourcing/offshoring data management responsibilities, APRA Prudential Standards, which deal specifically with this area, would apply to insurance companies who plan to outsource material business activities. The key requirements of the Prudential Standard are  
that an APRA-regulated institution must:

have a policy, approved by their board, relating to outsourcing of material business activities

have sufficient monitoring processes in place to manage the outsourcing of material business activities

for all outsourcing of material business activities with third parties, have a legally binding agreement in place, unless otherwise agreed by APRA

consult with APRA prior to entering into agreements to outsource material business activities to service providers that conduct their activities outside Australia

notify APRA after entering into agreements to outsource material business activities

## Do insurance companies have to ensure third parties meet certain standards in outsourcing processing to third parties? Are there additional safeguards to be taken?

See response to question 16 above.

APRA Standards applicable to insurance companies expects that a regulated entity would be able to demonstrate the following:

ability to continue operations and meet core obligations following a loss of services

maintenance of the quality of critical or sensitive data

compliance with legislative and prudential requirements

a lack of impediments (from jurisdictional hurdles or technical complications) to APRA being able to fulfill its duties as prudential regulator (including timely access to data in a usable form)

## What is the data retention requirement?

There are no specific data retention requirements under Australian privacy law, though we note that organizations should only retain personal data for as long as it is required to be used for the primary purpose for which it was collected.

## Are there regulatory requirements to have local data centers and disaster recovery processes?

While not a strict legal or regulatory requirement, OAIC guidelines and APRA Prudential Practice Guides indicate the importance of adequate disaster recovery processes as part of an organization's robust IT, cybersecurity and privacy management systems.

## What are the consequences of a data privacy breach? Is it a criminal offense? What is the penalty?

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (Privacy Amendment Act) which will take effect on 23 Feb 2018, will require certain “eligible” data breaches to be notified to the OAIC and affected individuals in accordance with that Act.

Failing to comply with the Privacy Amendment Act would be an "interference with the privacy of an individual," which may amount to a breach of a civil penalty provision of the Privacy Act. The main consequences include the risk of a determination to pay compensation and also the risk of paying civil penalties of an amount up to AUD 2.1 million (for corporations) and AUD 420,000 (for individuals).

## Is there a statutory obligation to disclose data breaches to regulators?

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

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

Preparing a statement setting out the entity’s identity and contact details, a description of the breach, the kind of information concerned and recommendations about what the affected individuals should do in response.

Giving a copy of the statement to the Australian Information Commissioner.

If practicable, taking reasonable steps to notify the contents of the statement to each individual to whom the relevant information relates, or, if it is not practicable to do so, to the individuals who are "at risk" of serious harm from the breach. An entity might choose  
to notify a statement under the first option where it would require an unreasonable amount of resources to assess which affected individuals are “at risk” from an eligible data breach and which are not. On the other hand, the second option may be more practicable  
if an entity is able to ascertain with a high degree of confidence that only some particular individuals are “at risk” from the eligible data breach.

If neither of the above methods are practicable, the entity must publish the statement on its website and take reasonable steps to publicize its content.

## Is there a statutory obligation to disclose data breaches to data owners?

Yes, see response to question 21. The notification obligations require notification to be made to both the OAIC and affected individuals.

## What are the statutory obligations to cooperate with regulators if there is a data breach?

See response to question 21 above.

## Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

Yes, CERT Australia provides a range of services, including a hotline, email support, technical guidance on mitigating cyber threats, incident response support and coordination, information sharing and capability building.

## Are there additional consequences which apply in the event of a data privacy breach under cybersecurity laws?

No, the Privacy Amendment Act sets out the primary obligations which apply in the event of a data breach in Australia.

# Digitalization in Insurance Guide

## Is there any specific regulation governing the sale of insurance through online platforms?

No. The law in Australia is 'technology neutral' (ASIC RG 255.6). To sell insurance that includes digital advice (digital advice is automated financial product advice using algorithms without the direct involvement of a human advisor) the insurer must obtain a license to do so and must act within the terms of that license (as must its authorised representatives). To the extent that the sale of insurance involves the provision of digital advice, or hybrid advice, the Regulator (Australian Securities and Investment Commission aka. **ASIC**) has issued Regulatory Guide (**RG**) 10.255.

## Is the sale of insurance through mobile applications subject to the same requirements as the online sale?

Yes.

## Set out three key regulatory requirements for the distributions of products online or through mobile applications.

If selling "digital advice" (i) there is an obligation that there be people within the business who have an understanding of the technology and algorithms used to provide the digital advice, and are able to review the digital advice generated by the algorithms (RG 255.61; RG 255.110-RG.113) (ii) The licensee must have sufficient technological resources to maintain client records and data integrity, protect confidential information, meet current and anticipated needs including in relation to system capacity, and have adequate business continuity, backup and disaster recovery plans for any systems that support the delivery of digital advice. The licensee must comply with all legal obligations (RG 255.66 and 255.67) and, if there is an outsourcing of functions that relate to the digital advice business there must be (iii) measures in place to ensure due skill and care is taken in choosing the service provider and to monitor the ongoing performance of that provider.

## Do the current insurance regulations in your jurisdiction allow the KYC process be done online or electronically? If so, what are the key requirements?

The law in Australia is 'technology neutral' (ASIC RG 255.6) and the Know Your Client obligations are set out in the Corporations Act 2001 and other legislation and guidelines.

## Do the insurance regulations permit insurance policies/contracts to be concluded through digital means? For example, through a “click-through” or “e-signature”, without any wet signature.

The law in Australia is 'technology neutral' so the same requirements for the inception of a policy apply as they would if not digital in nature. It is a matter for the digital license holder to ensure that verification is compliant.

Section 10 of the Electronic Transactions Act 1999 (Cth) governs the use of electronic payments and provides the requirements to be met in place of a signature.

## Is there any specific regulation governing the advertising of insurance products through online platforms or the use of aggregators?

No. The Corporations Act 2001 and the Australian Consumer Law govern misleading statements and the disclosures that are required of all insurance products irrespective of being online or not.

## Are there any customer service requirements if the insurers sell their products online?

No. Customer service requirements are the same as if the products were not sold online. The risk management framework however, of the AFSL holder must take into account the risk of hacking, cloud storage and confidentiality which are all matters that are the subject of regulatory guidelines under the Corporations Act 2001, ASIC and APRA guidelines.

## If an obligation is imposed on insurers to allow customers to amend or update their policies online, are there any specific regulatory requirements governing that process?

The process is not regulated but the ability to amend and update policies is dependant on the type of insurance product that is being sold and the legislation that governs it. Commonly, there are obligations upon insureds to disclose matters that are relevant to the insurer's decision to insure them and that may materially affect the risk insured.

## Are insurers required to apply for specific insurance licenses in order to conduct online sales?

Where digital advice is being provided of a personal nature, it is expected that the regulator will require disclosure of this and that licenses will be required for this.

## In order to conduct online sales, are insurance intermediaries required to apply for any specific insurance licenses?

No. Insurance intermediaries must act within the terms of the AFSL holder's license and to the extent that this does not occur, the AFSL holder will be liable. There will usually be indemnities contained in the agreement between the AFSL licensee and the intermediary (Authorised Representative) that reimburse the AFSL holder for any damages or compensation arising from the breaches of the Authorised Representative (intermediary).

## Are there specific requirements on the commission rates paid to insurance intermediaries for online sales? Please specify if these rates are different from the rates applicable in the case of insurance sale through other means.

There are no specific requirements.

## Where the insurers do not engage in online insurance sales themselves, but engage intermediaries to do so, would the insurers be deemed as offering or selling insurance products online?

Yes. The AFS licensee who outsources functions remains responsible for the financial services provided (RG 255.70) and licensees are liable for the acts of their authorised representatives (Corporations Act 2001 (Cth) sections 917A-F).

©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.