Cloud Compliance Center - Australia

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

**Australia**

*This content was last reviewed around April 2023.*

**Cloud friendly**

**1. Are financial institutions legally permitted to use cloud services?**

Yes, if the institution meets all applicable legal requirements for the use of cloud services.

**2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?**

Yes.

**Australian Prudential Regulation Authority ("APRA") Prudential Standards and Guidance**

Several mandatory Prudential Standards apply to entities regulated by the APRA, such as authorized deposit-taking institutions, superannuation funds and insurers (APRA-regulated entities). The Prudential Standards contain requirements relevant to outsourcing and data security. For example, banking, insurance and life insurance APRA-regulated entities are subject to Prudential Standard CPS 231 on Outsourcing ("**CPS 231**"). CPS 231 requires that outsourcing of "material business activities" be subject to appropriate due diligence, approval and ongoing monitoring. The APRA has also provided the following related guidance:

Prudential Practice Guide PPG 231 — Outsourcing, which indicates the APRA's view of sound practices for outsourcing and provides guidance on the implementation of CPS 231 (e.g., the usual content of the minimum contractual provisions for an outsourcing agreement)

Information Paper on Outsourcing Involving Cloud Computing Services, which outlines the APRA's expectations when applying the above requirements in a cloud computing context

Readers should note that a draft Prudential Standard CPS 230 on Operational Risk Management, which is intended to replace a range of prudential standards including CPS 231 from 2024, was the subject of consultation with industry stakeholders in 2022 and is planned to take effect from 2024.

There are also other Prudential Standards and guidance relating to information security risks that would be relevant when engaging a cloud services provider, primarily:

Prudential Standard CPS 220 on Risk Management — with additional guidance in Prudential Practice Guide CPG 220 on Risk Management

Prudential Standard CPS 234 on Information Security — with additional guidance in Prudential Practice Guide CPG 234 on Information Security

Prudential Practice Guide CPG 235 on Managing Data Risk — with additional guidance in Prudential Practice Guide CPG 235 on Managing Data Risk.

**Australian Securities and Investments Commission ("ASIC") requirements**

Entities that are Australian financial services licensees and Australian credit licensees will need to comply with the ASIC policy on the requirements for outsourcing to ensure they meet the competency requirements of their license conditions.

Additionally, from 10 March 2023, financial markets and participants of such markets are subject to updated ASIC market integrity rules containing enhanced technological and operational resilience requirements, including in relation to outsourcing.

**Exchange rules**

Entities that are participants with the Australian Securities Exchange ("**ASX**") and ASX Clear (the clearinghouse for all shares, structured products, warrants and ASX equity derivatives) will be subject to the ASX Operating Rules and ASX Clear Operating Rules, which include various requirements, including an obligation to notify the ASX in writing about details of material offshoring and outsourcing arrangements in respect of business activity conducted as a participant.

**3. Are there any specific contractual requirements for cloud outsourcing?**

**Australian Prudential Regulation Authority ("APRA") Prudential Standards and Guidance**

Where an APRA-regulated entity will be outsourcing a "material business activity," Prudential Standard CPS 231 ("**CPS 231**") on Outsourcing imposes requirements regarding the outsourcing agreement. For example:

The agreement must be signed before the outsourcing arrangement commences.

The entity must notify the APRA as soon as possible and no later than 20 business days after entering into the agreement and provide a key risks summary and details of risk minimization strategies in place.

The entity must consult with the APRA before entering into any offshoring agreement (the APRA may intervene and require the entity to make other arrangements).

The outsourcing agreement must address certain minimum matters. Notably, this includes the following:

The form in which data is to be kept and clear provisions identifying ownership and control of data

Liability and indemnity provisions, including an indemnity making the outsourced service provider liable for any subcontractor's failure

Business continuity management

Confidentiality, privacy and security of information

To the extent applicable, offshoring arrangements (including through subcontracting)

A clause allowing the APRA access to documentation and information related to the outsourcing arrangement

The entity must make notifications on termination of the outsourcing agreement.

Draft Prudential Standard CPS 230 on Operational Risk Management, which is planned to replace CPS 231 from January 2024, proposes some key changes to the above requirements.

**Australian Securities and Investments Commission ("ASIC") requirements**

From 10 March 2023, financial markets and participants of such markets are subject to updated ASIC market integrity rules containing enhanced technological and operational resilience requirements, including in relation to outsourcing. Requirements for outsourcing arrangements for critical business services include that the outsourcing agreement is documented and legally binding and the following:

It describes the nature, scope and quality of the services.

It requires notice of subcontracting or material service changes to be given to the operator.

It deals with termination and provides for orderly transition following termination.

It provides for the orderly transfer of services provided under the outsourcing arrangement to the operator/participant or another service provider in the event of termination of the outsourcing agreement.

**4. When does cloud outsourcing fall within the scope of the rules?**

**Australian Prudential Regulation Authority ("APRA") Prudential Standards and Guidance**

Under Prudential Standard CPS 231 on Outsourcing ("**CPS 231**"), an outsourcing will involve a "material business activity" if it "has the potential, if disrupted, to have a significant impact on the APRA-regulated institution's or group's business operations or its ability to manage risks effectively" having regard to various factors, including the following:

Financial, reputational and operational impact of a service provider failure over a given period

Cost of the arrangement

Degree of difficulty in finding an alternative service provider or bringing the activity in-house

Ability of the APRA-regulated entity or its affiliates to meet regulatory requirements if there are problems with the service provider

Additionally, Prudential Practice Guide PPG 231 — Outsourcing, indicates that the outsourcing of a significant part of a regulated institution's IT functions supporting its core business will be the outsourcing of a "material business activity." The APRA's notification and consultation expectations under CPS 231 turn on whether a particular arrangement involves low, heightened or extreme inherent risk, and the APRA's Information Paper on Outsourcing Involving Cloud Computing Services provides guidance on when a particular outsourcing will fall within these characterizations.

Prudential Standard CPS 220 on Risk Management and Prudential Standard CPS 234 on Information Security, sets general risk management and information security requirements for APRA-regulated entities. Additionally, Prudential Practice Guide CPG 234 on Information Security and Prudential Practice Guide CPG 235 on Managing Data Risk, provides guidance on information security and managing data risk, respectively. These requirements and guidance are not specific to cloud but nevertheless inform the basis on which such entities organize their data and information security arrangements and engage with third-party service providers such as cloud service providers.

Draft Prudential Standard CPS 230 on Operational Risk Management, which is intended to replace CPS 231 from January 2024, will have implications for cloud outsourcing arrangements. For example, the draft includes a non-exhaustive list of the services that would be classified as "material."

**Australian Securities and Investments Commission ("ASIC") requirements**

The enhanced technological and operational resilience requirements in the ASIC market integrity rules, which apply from 10 March 2023, apply in relation to outsourcing of "critical business services" meaning functions, infrastructure, processes or systems that in the event of failureto operate effectively would likely to cause significant disruption to a market participant's participant operations or to materially impact the participant's participant services. Notes to the rules indicate that this would generally include functions, infrastructure, processes and systems that deliver or support order acceptance, routing and entry, clearing and settlement of transactions, payments and deliveries of financial products and funds, accounting for or reconciling client money, trust accounts, securities and funds, confirmations and regulatory data reporting.

**Australian Securities Exchange ("ASX") rules**

Whether exchange rules impact the use of a cloud provider's services depends on the extent to which the outsourcing to the cloud service provider impacts upon the entity's interaction with the ASX. In this context, an arrangement is material if it constitutes the outsourcing of a material business activity. Examples include the outsourcing of the operation of core IT systems used in the participant's activities with the ASX and the outsourcing of the settlement and clearing function.

**5. Does the outsourcing need to be notified to the regulator?**

Yes, there are notification requirements that may apply depending on the type of entity, the nature of the outsourcing and other circumstances:

**Australian Prudential Regulation Authority ("APRA") Prudential Standards and Guidance**

Where an APRA-regulated entity will be outsourcing a "material business activity," Prudential Standard CPS 231 on Outsourcing ("**CPS 231**") imposes the following requirements for the entity (or the head of its group):

Notify the APRA as soon as possible and no later than 20 business days after entering into the outsourcing agreement, and provide a key risks summary and details of risk minimization strategies in place.

Consult with the APRA if offshoring to a service provider outside Australia.

Advise the APRA of any significant problems that have the potential to materially affect the outsourcing arrangement and, therefore, materially affect the business operations, profitability or reputation of the group.

Make notifications on the termination of the outsourcing agreement.

Additionally, the APRA may request the external auditor of an institution, or an appropriate external expert, to assess the entity's risk management processes with respect to the outsourcing of a material business activity.

Draft Prudential Standard CPS 230 on Operational Risk Management, which is planned to replace CPS 231 from January 2024, proposes to impose new requirements to notify the APRA as soon as possible, and not later than within 72 hours of becoming aware of a material operational risk incident.

The APRA Information Paper on Outsourcing Involving Cloud Computing Services also "encourages" consultation with the APRA prior to entering into any arrangement (regardless of whether offshoring is involved) when the proposed arrangement involves heightened or extreme inherent risks. There is guidance in the paper as to when this will be the case.

The general notification requirements of Prudential Standard CPS 220 on Risk Management ("**CPS 220**") and Prudential Standard CPS 234 on Information Security ("**CPS 234**") (and associated guidance) will also need to be considered when using a cloud services provider. For example, among other things:

CPS 220 imposes obligations to provide the APRA with copies of an entity's risk appetite statement, business plan and risk management strategy. It also requires an entity to notify the APRA on becoming aware of a significant breach of, or material deviation from, the risk management framework, or that the risk management framework does not adequately address a material risk.

CPS 234 imposes obligations to notify the APRA of certain material information security incidents, and of certain material information security control weaknesses, and this would need to be accounted for in third-party cloud service provider engagements.

**Australian Securities Exchange ("ASX") requirements**

As noted above, entities that are participants with the ASX and ASX Clear must comply with a notification requirement for the offshoring and outsourcing of material business activities with the ASX.

**6. What are the potential consequences for breaching financial services rules on cloud outsourcing?**

A breach of Australian Prudential Regulation Authority ("**APRA**") Prudential Standards constitutes a breach of the relevant underlying legislation for which the Prudential Standards apply, i.e., for banks, the Banking Act 1959 (Cth); for Australian financial services licensees, the Corporations Act 2001 (Cth); and for Australian credit licensees, the Credit Code.

Breach of this legislation can give rise to the following:

Criminal and civil action — Although a breach of the outsourcing requirements for cloud services is unlikely to be considered a conduct that constitutes an offense or would give rise to a civil penalty or infringement notice.

Administrative action — Both the APRA and the Australian Securities and Investments Commission ("**ASIC**") have a range of administrative remedies where they consider that a licensee is not meeting its obligations under the Prudential Standards, including removal of a license, additional conditions on the licensee, enforceable undertakings to remedy compliance breakdowns and banning orders for individuals.

For breaches of Australian Securities Exchange ("**ASX**") and ASX Clear Operating Rules, the consequences include warnings, additional conditions on the right to participate, additional capital requirements and independent expert reviews. For serious breaches, the remedies include fines, suspension or termination of participant rights and referral to the ASIC.

**7. Are there any data privacy and/or data security laws that would apply?**

Yes. The handling of personal information by private sector entities in Australia is regulated at a federal level by the Privacy Act 1988 (Cth) ("**Privacy Act**"). The key requirements for handling personal information are set out in the Australian Privacy Principles in Schedule 1 of the Privacy Act. Other notable features of the Privacy Act are the mandatory data breach notification obligations under Part IIIC, and special requirements for handling certain types of data (e.g., Part IIIA of the Privacy Act and the Credit Reporting Coderegulate the handling of credit-related personal information; the Privacy (Tax File Number) Rule 2015 regulates the handling of tax file numbers). These requirements apply irrespective of whether personal information is held or processed in cloud services, or otherwise, and are not specific to financial institutions.

The Privacy Act has been recently reviewed and the government is considering making a range of modernizations to Australian privacy law in response. This may ultimately lead to extensive changes to the Privacy Act and how personal information is regulated in Australia.

Additional requirements apply in respect of data that forms part of the Consumer Data Right scheme.

Furthermore, the Security of Critical Infrastructure Act (Cth) ("**SCIA**") includes the following features:

It applies to a range of sectors including communications, data storage and processing, and financial services.

It contains positive security obligations (including incident notification obligations) for owners and operators of critical infrastructure assets in these sectors, subject to a ministerial determination being made.

It includes enhanced cybersecurity obligations for designated "systems of national significance."

It provides the government with powers to direct owners and operators of critical infrastructure to provide information and do things in response to cybersecurity incidents, and to intervene in certain circumstances.

This could have indirect impacts for customers of cloud service providers who fall within the SCIA's regime (e.g., a cloud service provider could be subject to government investigations or interventions in response to cybersecurity incidents, and this may impact systems or data used to support its cloud services customers).

**8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?**

There are generally no applicable data localization requirements in Australia at present. However, there are some data protection requirements that need to be considered when offshoring data.

Where personal information is to be hosted in a data center outside Australia, the following Australian Privacy Principles ("**APPs**") contained in the Privacy Act 1988 (Cth) ("**Privacy Act**") will be relevant:

**APP 6:** If an entity regulated by the Privacy Act ("regulated entity") holds information about an individual that was collected for a particular purpose, that information must not be used or disclosed for another secondary purpose unless the relevant individual has consented to this, or the use or disclosure falls within one of a permitted set of exceptions. One such exception is where the individual would reasonably expect the entity to use or disclose the information for the secondary purpose and that secondary purpose is sufficiently related to the primary purpose of collection.

**APP 8.1:** Unless an exception applies, a regulated entity that is to disclose personal information to an overseas recipient must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs. The Australian-regulated entity is also subject to strict liability for breaches by the offshore entity. "Reasonable steps" in this context should include, at a minimum, having an appropriate data transfer agreement in place that obliges the offshore recipient to comply with the APPs and that also contains obligations framed to help ensure compliance in practice (e.g., audit rights and controls).

**APP 11:** A regulated entity must take reasonable steps to protect information from misuse, interference and loss, and from unauthorized access, modification or disclosure.

Specific to the cloud, the APPs provide guidance on when providing personal information to a cloud service provider might — in certain limited circumstances — be classified as a "use" by the regulated entity providing the information as opposed to a "disclosure" by the regulated entity. As such, it is possible that a pure cloud hosting arrangement that meets the above criteria may be classified as a use only, not a disclosure, by the customer and, therefore, will not be subject to APP 8. However, where no disclosure has occurred, the activity would still involve "use" and "holding" of the data by the cloud customer, hence APP 6 and APP 11 would still need to be complied with.

Additional requirements apply for data that is part of the Consumer Data Right scheme.

The Privacy Act has been recently reviewed and the government is considering making a range of modernizations to Australian privacy law in response, including proposals that would impact APP 6, APP 8 and APP 11. Any resulting changes to the law may have implications for the overseas hosting of data.

**9. Does a cloud service provider need a financial services authorization or license to provide cloud services?**

No, unless they constitute regulated activities in themselves.

**10. Is express consent from customers or other data subjects required before moving data to the cloud?**

Australian privacy law generally only requires an individual's consent to be obtained in certain limited circumstances (e.g., where an Australian-regulated entity wishes to use or disclose personal information for a secondary purpose that does not fall within any of the exceptions in Australian Privacy Principle ("**APP**") 6).

It would be unusual for a new express consent to be required in order to move an individual's personal information to a cloud service provider because any disclosure of data to a cloud service provider for a back-end purpose would likely be permitted on another basis under APP 6 (e.g., because it is for a related secondary purpose that the individual would reasonably expect, or potentially because there are reasonable grounds for implying consent in the circumstances, strengthened by disclosures already made and consent already obtained via existing privacy policies, collection notices and customer terms).

Obtaining consent from relevant individuals is also currently one of the exceptions to the overseas disclosure obligations in APP 8 (there are proposals to remove this exception). However, the requirements for obtaining a valid consent for such purposes are quite onerous and it would be unusual, in the context of a cloud services implementation, to seek express consent just for the purpose of obtaining an exception to APP 8.

The Privacy Act 1988 (Cth) ("**Privacy Act**") has recently been reviewed and legislative changes that ultimately result from the review may have some implications for cloud outsourcing arrangements. For example, the report on the review of the Privacy Act proposed some revisions to the law on overseas disclosures of personal information, such as changes to the consent exception to APP 8 and the introduction of standard contractual clauses that could be used to facilitate overseas disclosures.

Additional requirements apply for data that is part of the Consumer Data Right scheme.

**11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?**

If the entity or the data is in Australia, then the cloud service provider could be subject to Australian subpoenas/warrants, etc., in the normal way.

However, in terms of particularly onerous/out of the ordinary Australian requirements, Part 15 of the Telecommunications Act 1997 (Cth) ("**Telco Act**") enables relevant law enforcement agencies to issue various requests and orders to "designated communications providers," including the following:

Technology assistance requests (requesting voluntary assistance)

Technology assistance notices (requiring certain types of assistance to law enforcement agencies)

Technology capability notices (these could be used to compel a designated communications provider to build new capabilities to enable assistance)

There are some limitations on this (e.g., see Section 317ZG of the Telco Act), but the acts or things that a designated communications provider could be required to do could be broad; there is a long list in the legislation that includes removing one or more forms of electronic protection. This could also potentially include building a capability to provide access to encrypted communications and data.

"Designated communications providers" include the following:

A service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service

An electronic service that has one or more end users in Australia

A service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end users in Australia

A person who develops, supplies or updates software used, for use, or likely to be used, in connection with the following:

A listed carriage service

An electronic service that has one or more end users in Australia

**12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?**

Potentially, yes. See the response to question 11 regarding legal requirements to provide access to data.

Additionally, in 2021, the Telecommunications Legislation Amendment (International Production Orders) Act 2021 (Cth) ("**IPO Act**") came into effect, establishing a legislative framework for Australia to enter into future bilateral and multilateral agreements for cross-border access to communications data.

The IPO Act is broad in scope and could provide the basis for foreign law enforcement to access data held or processed by a cloud service provider for a financial institution, in response to an international production order. This legislation sets the stage for Australia to enter into bilateral agreements with other countries, enabling government agencies in both countries to request access to certain communications data held by service providers located in the other country, for law enforcement and national security purposes. Australia concluded such an agreement with the US in late 2021.

Further, under the Security of Critical Infrastructure Act 2018(Cth), responsible entities for critical infrastructure in the communications, data storage and processing, and financial services sectors are also required (among other things) to disclose certain information in response to cybersecurity incidents. These entities can also be subject to information-gathering directions, action directions or intervention requests in the event of an incident that could result in further information needing to be provided or made accessible to the government. Additionally, owners and operators of designated systems of national significance have additional enhanced cybersecurity obligations that may include providing the government with access to systems information.

# Permissibility of cloud

## 1. Are financial institutions legally permitted to use cloud services?

Yes, if the institution meets all applicable legal requirements for the use of cloud services.

# Rules for cloud outsourcing

## 2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?

Yes.

**Australian Prudential Regulation Authority ("APRA") Prudential Standards and Guidance**

Several mandatory Prudential Standards apply to entities regulated by the APRA, such as authorized deposit-taking institutions, superannuation funds and insurers (APRA-regulated entities). The Prudential Standards contain requirements relevant to outsourcing and data security. For example, banking, insurance and life insurance APRA-regulated entities are subject to Prudential Standard CPS 231 on Outsourcing ("**CPS 231**"). CPS 231 requires that outsourcing of "material business activities" be subject to appropriate due diligence, approval and ongoing monitoring. The APRA has also provided the following related guidance:

Prudential Practice Guide PPG 231 — Outsourcing, which indicates the APRA's view of sound practices for outsourcing and provides guidance on the implementation of CPS 231 (e.g., the usual content of the minimum contractual provisions for an outsourcing agreement)

Information Paper on Outsourcing Involving Cloud Computing Services, which outlines the APRA's expectations when applying the above requirements in a cloud computing context

Readers should note that a draft Prudential Standard CPS 230 on Operational Risk Management, which is intended to replace a range of prudential standards including CPS 231 from 2024, was the subject of consultation with industry stakeholders in 2022 and is planned to take effect from 2024.

There are also other Prudential Standards and guidance relating to information security risks that would be relevant when engaging a cloud services provider, primarily:

Prudential Standard CPS 220 on Risk Management — with additional guidance in Prudential Practice Guide CPG 220 on Risk Management

Prudential Standard CPS 234 on Information Security — with additional guidance in Prudential Practice Guide CPG 234 on Information Security

Prudential Practice Guide CPG 235 on Managing Data Risk — with additional guidance in Prudential Practice Guide CPG 235 on Managing Data Risk.

**Australian Securities and Investments Commission ("ASIC") requirements**

Entities that are Australian financial services licensees and Australian credit licensees will need to comply with the ASIC policy on the requirements for outsourcing to ensure they meet the competency requirements of their license conditions.

Additionally, from 10 March 2023, financial markets and participants of such markets are subject to updated ASIC market integrity rules containing enhanced technological and operational resilience requirements, including in relation to outsourcing.

**Exchange rules**

Entities that are participants with the Australian Securities Exchange ("**ASX**") and ASX Clear (the clearinghouse for all shares, structured products, warrants and ASX equity derivatives) will be subject to the ASX Operating Rules and ASX Clear Operating Rules, which include various requirements, including an obligation to notify the ASX in writing about details of material offshoring and outsourcing arrangements in respect of business activity conducted as a participant.

# Contract requirements

## 3. Are there any specific contractual requirements for cloud outsourcing?

**Australian Prudential Regulation Authority ("APRA") Prudential Standards and Guidance**

Where an APRA-regulated entity will be outsourcing a "material business activity," Prudential Standard CPS 231 ("**CPS 231**") on Outsourcing imposes requirements regarding the outsourcing agreement. For example:

The agreement must be signed before the outsourcing arrangement commences.

The entity must notify the APRA as soon as possible and no later than 20 business days after entering into the agreement and provide a key risks summary and details of risk minimization strategies in place.

The entity must consult with the APRA before entering into any offshoring agreement (the APRA may intervene and require the entity to make other arrangements).

The outsourcing agreement must address certain minimum matters. Notably, this includes the following:

The form in which data is to be kept and clear provisions identifying ownership and control of data

Liability and indemnity provisions, including an indemnity making the outsourced service provider liable for any subcontractor's failure

Business continuity management

Confidentiality, privacy and security of information

To the extent applicable, offshoring arrangements (including through subcontracting)

A clause allowing the APRA access to documentation and information related to the outsourcing arrangement

The entity must make notifications on termination of the outsourcing agreement.

Draft Prudential Standard CPS 230 on Operational Risk Management, which is planned to replace CPS 231 from January 2024, proposes some key changes to the above requirements.

**Australian Securities and Investments Commission ("ASIC") requirements**

From 10 March 2023, financial markets and participants of such markets are subject to updated ASIC market integrity rules containing enhanced technological and operational resilience requirements, including in relation to outsourcing. Requirements for outsourcing arrangements for critical business services include that the outsourcing agreement is documented and legally binding and the following:

It describes the nature, scope and quality of the services.

It requires notice of subcontracting or material service changes to be given to the operator.

It deals with termination and provides for orderly transition following termination.

It provides for the orderly transfer of services provided under the outsourcing arrangement to the operator/participant or another service provider in the event of termination of the outsourcing agreement.

# Regulated cloud outsourcing

## 4. When does cloud outsourcing fall within the scope of the rules?

**Australian Prudential Regulation Authority ("APRA") Prudential Standards and Guidance**

Under Prudential Standard CPS 231 on Outsourcing ("**CPS 231**"), an outsourcing will involve a "material business activity" if it "has the potential, if disrupted, to have a significant impact on the APRA-regulated institution's or group's business operations or its ability to manage risks effectively" having regard to various factors, including the following:

Financial, reputational and operational impact of a service provider failure over a given period

Cost of the arrangement

Degree of difficulty in finding an alternative service provider or bringing the activity in-house

Ability of the APRA-regulated entity or its affiliates to meet regulatory requirements if there are problems with the service provider

Additionally, Prudential Practice Guide PPG 231 — Outsourcing, indicates that the outsourcing of a significant part of a regulated institution's IT functions supporting its core business will be the outsourcing of a "material business activity." The APRA's notification and consultation expectations under CPS 231 turn on whether a particular arrangement involves low, heightened or extreme inherent risk, and the APRA's Information Paper on Outsourcing Involving Cloud Computing Services provides guidance on when a particular outsourcing will fall within these characterizations.

Prudential Standard CPS 220 on Risk Management and Prudential Standard CPS 234 on Information Security, sets general risk management and information security requirements for APRA-regulated entities. Additionally, Prudential Practice Guide CPG 234 on Information Security and Prudential Practice Guide CPG 235 on Managing Data Risk, provides guidance on information security and managing data risk, respectively. These requirements and guidance are not specific to cloud but nevertheless inform the basis on which such entities organize their data and information security arrangements and engage with third-party service providers such as cloud service providers.

Draft Prudential Standard CPS 230 on Operational Risk Management, which is intended to replace CPS 231 from January 2024, will have implications for cloud outsourcing arrangements. For example, the draft includes a non-exhaustive list of the services that would be classified as "material."

**Australian Securities and Investments Commission ("ASIC") requirements**

The enhanced technological and operational resilience requirements in the ASIC market integrity rules, which apply from 10 March 2023, apply in relation to outsourcing of "critical business services" meaning functions, infrastructure, processes or systems that in the event of failure to operate effectively would likely to cause significant disruption to a market participant's participant operations or to materially impact the participant's participant services. Notes to the rules indicate that this would generally include functions, infrastructure, processes and systems that deliver or support order acceptance, routing and entry, clearing and settlement of transactions, payments and deliveries of financial products and funds, accounting for or reconciling client money, trust accounts, securities and funds, confirmations and regulatory data reporting.

**Australian Securities Exchange ("ASX") rules**

Whether exchange rules impact the use of a cloud provider's services depends on the extent to which the outsourcing to the cloud service provider impacts upon the entity's interaction with the ASX. In this context, an arrangement is material if it constitutes the outsourcing of a material business activity. Examples include the outsourcing of the operation of core IT systems used in the participant's activities with the ASX and the outsourcing of the settlement and clearing function.

# Regulatory notifications

## 5. Does the outsourcing need to be notified to the regulator?

Yes, there are notification requirements that may apply depending on the type of entity, the nature of the outsourcing and other circumstances:

**Australian Prudential Regulation Authority ("APRA") Prudential Standards and Guidance**

Where an APRA-regulated entity will be outsourcing a "material business activity," Prudential Standard CPS 231 on Outsourcing ("**CPS 231**") imposes the following requirements for the entity (or the head of its group):

Notify the APRA as soon as possible and no later than 20 business days after entering into the outsourcing agreement, and provide a key risks summary and details of risk minimization strategies in place.

Consult with the APRA if offshoring to a service provider outside Australia.

Advise the APRA of any significant problems that have the potential to materially affect the outsourcing arrangement and, therefore, materially affect the business operations, profitability or reputation of the group.

Make notifications on the termination of the outsourcing agreement.

Additionally, the APRA may request the external auditor of an institution, or an appropriate external expert, to assess the entity's risk management processes with respect to the outsourcing of a material business activity.

Draft Prudential Standard CPS 230 on Operational Risk Management, which is planned to replace CPS 231 from January 2024, proposes to impose new requirements to notify the APRA as soon as possible, and not later than within 72 hours of becoming aware of a material operational risk incident.

The APRA Information Paper on Outsourcing Involving Cloud Computing Services also "encourages" consultation with the APRA prior to entering into any arrangement (regardless of whether offshoring is involved) when the proposed arrangement involves heightened or extreme inherent risks. There is guidance in the paper as to when this will be the case.

The general notification requirements of Prudential Standard CPS 220 on Risk Management ("**CPS 220**") and Prudential Standard CPS 234 on Information Security ("**CPS 234**") (and associated guidance) will also need to be considered when using a cloud services provider. For example, among other things:

CPS 220 imposes obligations to provide the APRA with copies of an entity's risk appetite statement, business plan and risk management strategy. It also requires an entity to notify the APRA on becoming aware of a significant breach of, or material deviation from, the risk management framework, or that the risk management framework does not adequately address a material risk.

CPS 234 imposes obligations to notify the APRA of certain material information security incidents, and of certain material information security control weaknesses, and this would need to be accounted for in third-party cloud service provider engagements.

**Australian Securities Exchange ("ASX") requirements**

As noted above, entities that are participants with the ASX and ASX Clear must comply with a notification requirement for the offshoring and outsourcing of material business activities with the ASX.

# Consequences of regulatory breach

## 6. What are the potential consequences for breaching financial services rules on cloud outsourcing?

A breach of Australian Prudential Regulation Authority ("**APRA**") Prudential Standards constitutes a breach of the relevant underlying legislation for which the Prudential Standards apply, i.e., for banks, the Banking Act 1959 (Cth); for Australian financial services licensees, the Corporations Act 2001 (Cth); and for Australian credit licensees, the Credit Code.

Breach of this legislation can give rise to the following:

Criminal and civil action — Although a breach of the outsourcing requirements for cloud services is unlikely to be considered a conduct that constitutes an offense or would give rise to a civil penalty or infringement notice.

Administrative action — Both the APRA and the Australian Securities and Investments Commission ("**ASIC**") have a range of administrative remedies where they consider that a licensee is not meeting its obligations under the Prudential Standards, including removal of a license, additional conditions on the licensee, enforceable undertakings to remedy compliance breakdowns and banning orders for individuals.

For breaches of Australian Securities Exchange ("**ASX**") and ASX Clear Operating Rules, the consequences include warnings, additional conditions on the right to participate, additional capital requirements and independent expert reviews. For serious breaches, the remedies include fines, suspension or termination of participant rights and referral to the ASIC.

# Data privacy and security

## 7. Are there any data privacy and/or data security laws that would apply?

Yes. The handling of personal information by private sector entities in Australia is regulated at a federal level by the Privacy Act 1988 (Cth) ("**Privacy Act**"). The key requirements for handling personal information are set out in the Australian Privacy Principles in Schedule 1 of the Privacy Act. Other notable features of the Privacy Act are the mandatory data breach notification obligations under Part IIIC, and special requirements for handling certain types of data (e.g., Part IIIA of the Privacy Act and the Credit Reporting Coderegulate the handling of credit-related personal information; the Privacy (Tax File Number) Rule 2015 regulates the handling of tax file numbers). These requirements apply irrespective of whether personal information is held or processed in cloud services, or otherwise, and are not specific to financial institutions.

The Privacy Act has been recently reviewed and the government is considering making a range of modernizations to Australian privacy law in response. This may ultimately lead to extensive changes to the Privacy Act and how personal information is regulated in Australia.

Additional requirements apply in respect of data that forms part of the Consumer Data Right scheme.

Furthermore, the Security of Critical Infrastructure Act (Cth) ("**SCIA**") includes the following features:

It applies to a range of sectors including communications, data storage and processing, and financial services.

It contains positive security obligations (including incident notification obligations) for owners and operators of critical infrastructure assets in these sectors, subject to a ministerial determination being made.

It includes enhanced cybersecurity obligations for designated "systems of national significance."

It provides the government with powers to direct owners and operators of critical infrastructure to provide information and do things in response to cybersecurity incidents, and to intervene in certain circumstances.

This could have indirect impacts for customers of cloud service providers who fall within the SCIA's regime (e.g., a cloud service provider could be subject to government investigations or interventions in response to cybersecurity incidents, and this may impact systems or data used to support its cloud services customers).

# Overseas hosting

## 8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?

There are generally no applicable data localization requirements in Australia at present. However, there are some data protection requirements that need to be considered when offshoring data.

Where personal information is to be hosted in a data center outside Australia, the following Australian Privacy Principles ("**APPs**") contained in the Privacy Act 1988 (Cth) ("**Privacy Act**") will be relevant:

**APP 6:** If an entity regulated by the Privacy Act ("regulated entity") holds information about an individual that was collected for a particular purpose, that information must not be used or disclosed for another secondary purpose unless the relevant individual has consented to this, or the use or disclosure falls within one of a permitted set of exceptions. One such exception is where the individual would reasonably expect the entity to use or disclose the information for the secondary purpose and that secondary purpose is sufficiently related to the primary purpose of collection.

**APP 8.1:** Unless an exception applies, a regulated entity that is to disclose personal information to an overseas recipient must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs. The Australian-regulated entity is also subject to strict liability for breaches by the offshore entity. "Reasonable steps" in this context should include, at a minimum, having an appropriate data transfer agreement in place that obliges the offshore recipient to comply with the APPs and that also contains obligations framed to help ensure compliance in practice (e.g., audit rights and controls).

**APP 11:** A regulated entity must take reasonable steps to protect information from misuse, interference and loss, and from unauthorized access, modification or disclosure.

Specific to the cloud, the APPs provide guidance on when providing personal information to a cloud service provider might — in certain limited circumstances — be classified as a "use" by the regulated entity providing the information as opposed to a "disclosure" by the regulated entity. As such, it is possible that a pure cloud hosting arrangement that meets the above criteria may be classified as a use only, not a disclosure, by the customer and, therefore, will not be subject to APP 8. However, where no disclosure has occurred, the activity would still involve "use" and "holding" of the data by the cloud customer, hence APP 6 and APP 11 would still need to be complied with.

Additional requirements apply for data that is part of the Consumer Data Right scheme.

The Privacy Act has been recently reviewed and the government is considering making a range of modernizations to Australian privacy law in response, including proposals that would impact APP 6, APP 8 and APP 11. Any resulting changes to the law may have implications for the overseas hosting of data.

# Financial services authorizations licenses

## 9. Does a cloud service provider need a financial services authorization or license to provide cloud services?

No, unless they constitute regulated activities in themselves.

# Customer data subject consent

## 10. Is express consent from customers or other data subjects required before moving data to the cloud?

Australian privacy law generally only requires an individual's consent to be obtained in certain limited circumstances (e.g., where an Australian-regulated entity wishes to use or disclose personal information for a secondary purpose that does not fall within any of the exceptions in Australian Privacy Principle ("**APP**") 6).

It would be unusual for a new express consent to be required in order to move an individual's personal information to a cloud service provider because any disclosure of data to a cloud service provider for a back-end purpose would likely be permitted on another basis under APP 6 (e.g., because it is for a related secondary purpose that the individual would reasonably expect, or potentially because there are reasonable grounds for implying consent in the circumstances, strengthened by disclosures already made and consent already obtained via existing privacy policies, collection notices and customer terms).

Obtaining consent from relevant individuals is also currently one of the exceptions to the overseas disclosure obligations in APP 8 (there are proposals to remove this exception). However, the requirements for obtaining a valid consent for such purposes are quite onerous and it would be unusual, in the context of a cloud services implementation, to seek express consent just for the purpose of obtaining an exception to APP 8.

The Privacy Act 1988 (Cth) ("**Privacy Act**") has recently been reviewed and legislative changes that ultimately result from the review may have some implications for cloud outsourcing arrangements. For example, the report on the review of the Privacy Act proposed some revisions to the law on overseas disclosures of personal information, such as changes to the consent exception to APP 8 and the introduction of standard contractual clauses that could be used to facilitate overseas disclosures.

Additional requirements apply for data that is part of the Consumer Data Right scheme.

# Data access requirements

## 11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?

If the entity or the data is in Australia, then the cloud service provider could be subject to Australian subpoenas/warrants, etc., in the normal way.

However, in terms of particularly onerous/out of the ordinary Australian requirements, Part 15 of the Telecommunications Act 1997 (Cth) ("**Telco Act**") enables relevant law enforcement agencies to issue various requests and orders to "designated communications providers," including the following:

Technology assistance requests (requesting voluntary assistance)

Technology assistance notices (requiring certain types of assistance to law enforcement agencies)

Technology capability notices (these could be used to compel a designated communications provider to build new capabilities to enable assistance)

There are some limitations on this (e.g., see Section 317ZG of the Telco Act), but the acts or things that a designated communications provider could be required to do could be broad; there is a long list in the legislation that includes removing one or more forms of electronic protection. This could also potentially include building a capability to provide access to encrypted communications and data.

"Designated communications providers" include the following:

A service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service

An electronic service that has one or more end users in Australia

A service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end users in Australia

A person who develops, supplies or updates software used, for use, or likely to be used, in connection with the following:

A listed carriage service

An electronic service that has one or more end users in Australia

# Data disclosure requirements

## 12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?

Potentially, yes. See the response to question 11 regarding legal requirements to provide access to data.

Additionally, in 2021, the Telecommunications Legislation Amendment (International Production Orders) Act 2021 (Cth) ("**IPO Act**") came into effect, establishing a legislative framework for Australia to enter into future bilateral and multilateral agreements for cross-border access to communications data.

The IPO Act is broad in scope and could provide the basis for foreign law enforcement to access data held or processed by a cloud service provider for a financial institution, in response to an international production order. This legislation sets the stage for Australia to enter into bilateral agreements with other countries, enabling government agencies in both countries to request access to certain communications data held by service providers located in the other country, for law enforcement and national security purposes. Australia concluded such an agreement with the US in late 2021.

Further, under the Security of Critical Infrastructure Act 2018 (Cth), responsible entities for critical infrastructure in the communications, data storage and processing, and financial services sectors are also required (among other things) to disclose certain information in response to cybersecurity incidents. These entities can also be subject to information-gathering directions, action directions or intervention requests in the event of an incident that could result in further information needing to be provided or made accessible to the government. Additionally, owners and operators of designated systems of national significance have additional enhanced cybersecurity obligations that may include providing the government with access to systems information.

©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.