Cloud computing and privacy

Small business factsheet

Australian Government
Department of Communications

enter

What is Cloud computing?

Cloud computing is the delivery of ICT services over the internet on demand. Consumers no longer need to buy, build or install expensive computer systems. Users can instead access computing resources as a utility service via a wired or wireless network – from the cloud. Cloud computing is already a major part of many people's lives. Services such as Google Maps, Apple iTunes, and webmail services including Gmail and Hotmail are all delivered through cloud computing.

Cloud computing can offer a range of benefits to small business by offering security improvements, cost savings, improved reliability, and access to services and data from multiple devices.

Privacy and the cloud

Some of the perceived risks associated with small business using the cloud often relate to issues of privacy. Like all ICT, using cloud computing is a question of taking advantage of the benefits while managing the potential risks.

This factsheet provides advice on how privacy legislation applies to cloud computing. It contains some privacy-related questions you may want to ask your cloud service provider to help you make an informed and confident decision for your business. In addition to providing information on how your business is protected when using the cloud, this factsheet also outlines your legislative obligations as a small business to protect personal information that may be in your care.

Legislative protections

In Australia, there are two key laws that provide protections when using cloud services. Even if your cloud provider is based overseas, these laws may still apply although they can be more difficult to enforce in these situations.

The Privacy Act 1988

The *Privacy Act 1988* (Privacy Act) regulates the handling of personal information by businesses with an annual turnover of more than $3 million, and certain smaller businesses including health service providers and businesses that trade in personal information[1].

Personal information is any information or opinion that identifies an individual[2]. This includes information that could be 'reasonably used' to identify someone, such as a telephone number in many cases. Businesses are subject to the obligations set out in the 'Australian Privacy Principles' or 'APPs'.

---

1 Further advice on entities covered by the privacy Act can be found on the OAIC website here.

2 This is a simplified definition. A complete definition can be found here on the OAIC's website.

There are some circumstances where the Privacy Act may not apply to your cloud service provider, for example when the cloud service provider is a small business with an annual turnover of less than $3 million. If you are in doubt, remember to ask your cloud service provider for details and shop around for the service that suits you best.

Businesses covered by the Privacy Act are subject to the obligations set out in the 'Australian Privacy Principles' or 'APPs'. The APPs generally apply to entities that hold personal information. In the context of cloud computing, key obligations include the following:

- The privacy policies of cloud providers must state the intended disclosure arrangements of personal information, including to any offshore storage destination/recipients (APP 1);
- Cloud providers can only disclose personal information to a person or organisation outside Australia where they have taken reasonable steps to ensure the overseas recipient does not breach the protections afforded under Australian privacy law. Further, cloud providers remain legislatively accountable for unauthorised or inadvertent data security breaches that may occur offshore (APP 8);
- Cloud providers must give an individual access to personal data held about them upon request – and take reasonable steps correct any personal data if required (APP 10, APP 12, APP 13);
- Cloud providers must take reasonable steps to secure personal data from misuse, interference or loss and from unauthorised access, modification or disclosure (APP 11);
- Cloud providers must take reasonable steps to delete or de-identify personal information that is no longer needed for the purpose for which it was collected (APP 11).

Remember that the Privacy Act may apply even if your provider is based overseas, and even if your contract with the provider says that a different law applies.

As a small business, even if you are not bound by the obligations in the Privacy Act, privacy should be an important consideration in dealing with your customer's information. Lack of adequate privacy protections could affect your business' reputation.

The Office of the Australian Information Commissioner (OAIC) is responsible for enforcing the Privacy Act. Further information on the protections within the Privacy Act, including how you can make a complaint for a suspected breach of the Act, can be found on the OAIC's website.

Australian Consumer Law

Small business consumers of the cloud remain protected by the overarching consumer protection framework that applies to all goods and services in Australia – the Australian Consumer Law (ACL). The ACL is technology neutral and provides protection against:

- false or misleading representations;
- unconscionable conduct; and
- product guarantees.

If a cloud service provider claims that a certain level of protection will apply to your data, and fails to live up to its promise, it might be in breach of the ACL. For more information about how the ACL might apply to a cloud service, have a look at the Legal tips for small businesses using cloud services factsheet, developed by the Department of Communications.

The ACL is enforced jointly by the Australian Competition and Consumer Commission (ACCC) and fair trading bodies in each state and territory. Further information on the ACL, including how to make a complaint, is available at www.consumerlaw.gov.au.

Key considerations for small business

By using a cloud service you will be entering into a contract. In most cases this contract will set out the obligations that the provider has committed to. As with most ICT services, a cloud computing contract may be 'standard form' with little opportunity to negotiate specific terms and conditions.

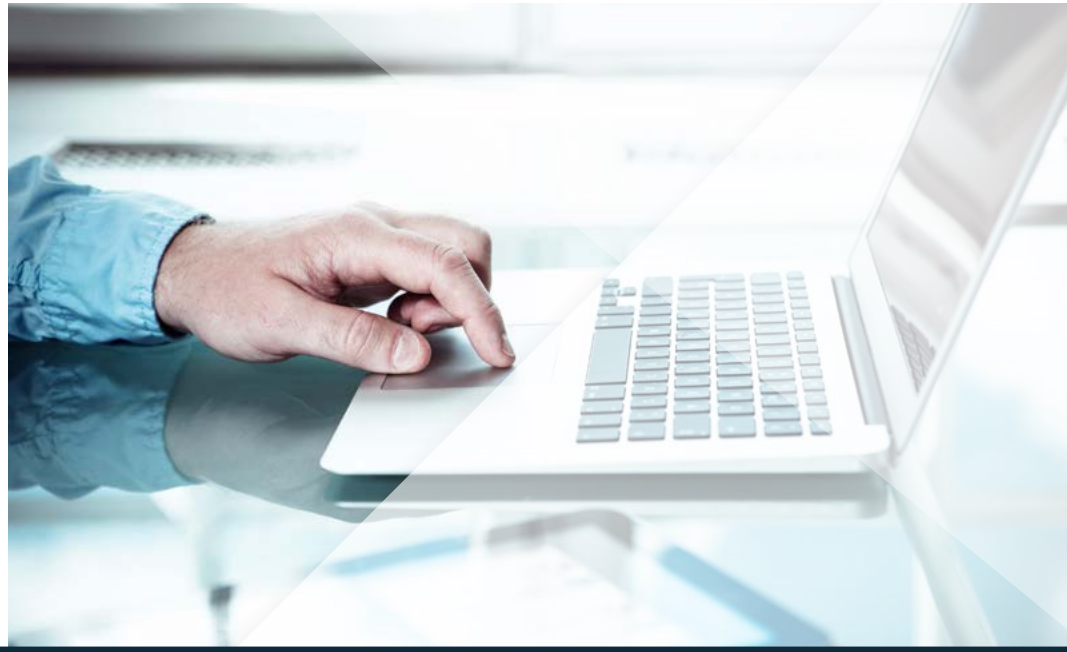
Before you agree to the terms and conditions, you should consider whether they satisfy your expectations and meet your specific business needs. This can be more important than comparing the price of two or more services. You should think about the specific needs that apply to the type of information you will be storing, the contractual details, and the privacy policies of the cloud service provider you are considering. It may be useful to discuss with a potential cloud service provider your data security needs to ensure that they will apply appropriate levels of protection to the information.

Before choosing a cloud service, shop around, compare services, read terms and conditions and ask your potential provider questions. For a more complete list of questions see Questions to ask your Cloud Provider.

Privacy specific questions you may wish to ask your cloud service provider include:

Where will my data be stored?

- If you, or your customers, have a preference for onshore storage options, your provider should be able to clearly inform you of the physical location of their intended data storage facilities. You should be aware that different countries have different laws that may allow access to stored data for purposes of law enforcement and national security.



Do you offer personalised encryption services for my data?

- Some cloud providers offer encryption services to give their customers an additional level of protection for their stored data. Encryption services may be offered as a standard feature, or as an additional feature (for a fee) upon request. Depending on your individual business needs, some cloud providers can provide you with direct access to your stored data at any time via secure and customised access interfaces to allow you to manage your data in real time.
- You should also be aware that some contractual terms may allow the cloud service provider, or a third party, to access your data.

Will my data be deleted after my contract expires?

- Some providers delete your data when your contract expires. Others will keep your data for reuse. You should also be aware that 'data anonymization' practices are not the same as 'data deletion' practices.
- You should also be mindful of contractual terms that seek to transfer ownership of your or your customer's data upon contract completion.

Do you back-up my data?

- Providers that back-up your data offer increased chances for the preservation of your data in the event of a security attack - or related problem. This is a particularly important safeguard if your business manages or stores data on behalf of third parties.

How will my data be provided to me (in what format) upon my contract expiration? What are your exit clauses if I choose to migrate to another vendor?

- Knowing how your data will be returned to you will help your small business transition to an alternative storage arrangement. Further, migrating to an alternative provider should also be an easy process and not complicated by complex contractual exit clauses.

Under what circumstances will data be disclosed to third parties?

- If you are uncomfortable with proposed disclosure arrangements, particularly where the express consent of you, or your business, isn't required, you can shop around for a more suitable provider.

Australian Government

Department of Communications

Disclaimer: This document provides factual information only and is not business or legal advice. You should seek professional advice before taking any action based on its contents.

back to start