Cloud computing and privacy

Consumer 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.

Privacy and the cloud

When it comes to cloud computing, privacy and security are key issues. This factsheet provides advice on how you can find out the extent to which your privacy is protected when using the cloud. It contains some privacy-related questions you may want to ask your cloud service provider to help you make an informed and confident decision.

Legislative protections

In Australia, there are two key laws that provide protection to consumers 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

The *Privacy Act 1988* (Privacy Act) regulates how most businesses handle personal information. Personal information is any information or opinion about an individual who is 'reasonably identifiable'[1]. This includes information that could be reasonably linked with an indiviudal's identity, such as a telephone number in many cases.

Businesses covered by the Privacy Act are subject to the obligations set out in the 'Australian Privacy Principles' or 'APPs'. The following examples should give you an idea of what to expect from businesses covered by the APPs that provide cloud services:

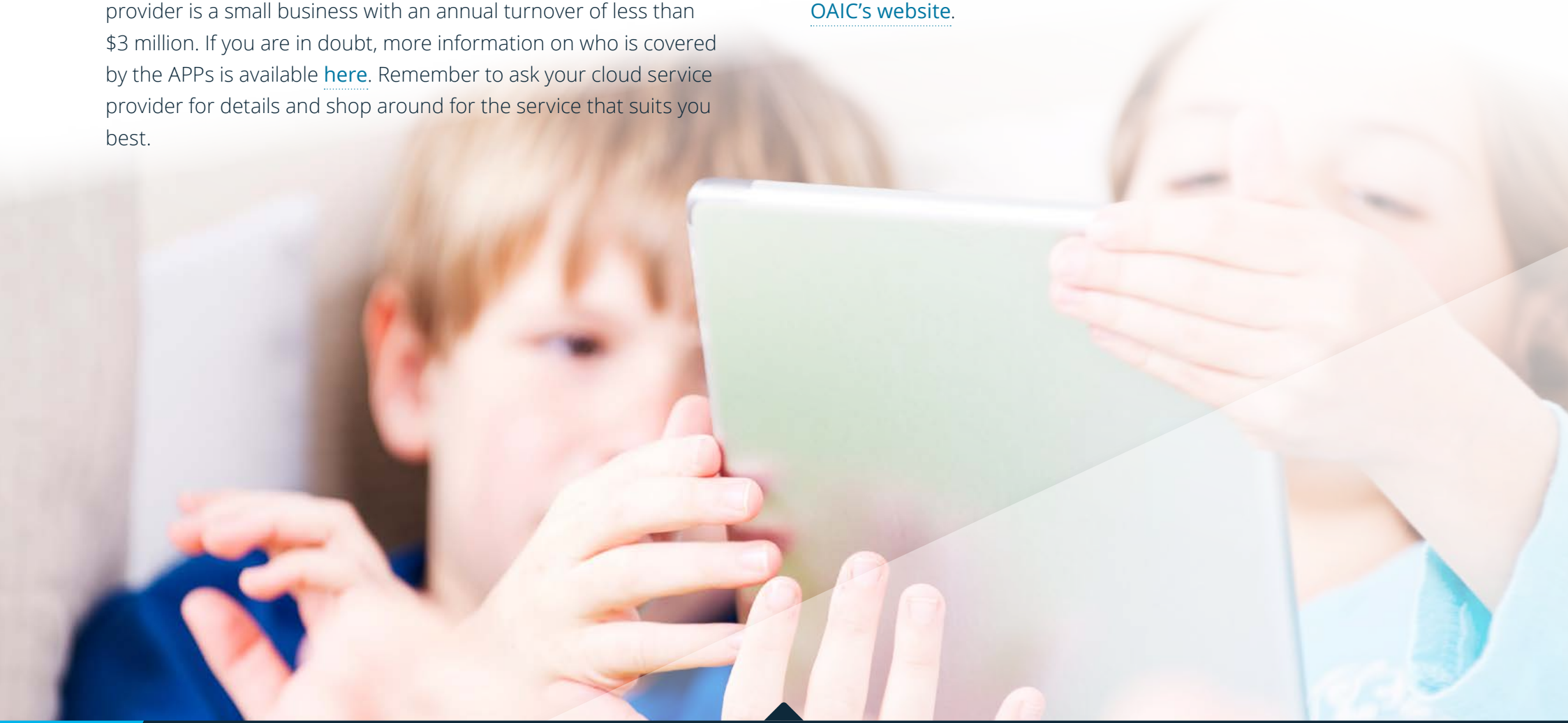
- The privacy policies of cloud providers must notify you as to what personal information will be collected and state the intended disclosure arrangements of personal information, including to any offshore storage destinations or recipients;
- Cloud providers can only disclose personal information outside of Australia where they have taken reasonable steps to ensure the overseas recipient does not breach the APPs (unless a listed exception applies);
- Cloud providers must give you access to your personal information upon request – and take reasonable steps to correct any incorrect personal information on request;
- Cloud providers must take reasonable steps to secure personal information from misuse, interference or loss and from unauthorised access, modification or disclosure, including security breaches that occur offshore; and
- 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.

---

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

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. However, there are some circumstances where the Privacy Act does not apply, 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, more information on who is covered by the APPs is available here. Remember to ask your cloud service provider for details and shop around for the service that suits you best.

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 (ACL)

When using a cloud service you are also broadly protected by the Australian Consumer Law (ACL). The ACL is technology neutral and provides consumers with protections against:

- unfair contractual terms and conditions;
- false or misleading representations;
- unconscionable conduct; and
- product guarantees.

For example, 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.

Questions to ask your cloud service provider

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.

Key privacy related questions include:

Where will my data be stored?

- If you 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.

Will you encrypt my data? Do you offer encryption services?

- Some cloud providers offer encryption services to give 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.

Will my data be deleted after my contract expires? If so, when?

- 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.

Do you back-up my data? If so, where is the back-up stored?

- Providers that back-up your data provide additional resilience in the event of data loss and offer increased chances for the preservation of your data in the event of a security attack.

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 you transition to an alternative arrangement. You should check whether migrating to an alternative provider will 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 your express consent 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