Applying the legislation

GUIDELINE – Information Privacy Act 2009

Cloud computing and the privacy principles

Overview

The Information Privacy Act 2009 (Qld) (IP Act) contains a number of privacy principles which set out the rules for how personal information is to be collected, managed, used and disclosed by Queensland government agencies.1

Personal information

Personal information is defined in section 12 of the IP Act. It is a broad definition that encompasses any information about an individual who can be identified directly from the information, or whose identity can be reasonably ascertained by reference to other information. Information does not have to be true, written down, sensitive or 'important' to be personal information.

What are the privacy principles?

The privacy principles are the obligations set out in chapter 2 of the IP Act. They include the obligation to comply with the Information Privacy Principles (IPPs) or, for health agencies, the National Privacy Principles (NPPs), the contracted service provider principles in part 4 and the rules about transferring personal information out of Australia in section 33.

What is cloud computing?

Cloud computing is not a new concept; webmail services, such as Hotmail which has been in operation since 1997, is an example of cloud computing. The phrase 'cloud computing' is simply a shorthand term for moving functions from a computer and agency-owned server to an online environment, for example, employees accessing word processing programs through a webpage interface instead of from the Programs menu on their computer. Computing power, storage space, applications and programs may all be outsourced to 'the cloud', i.e. a remote provider whose services are accessed via the internet.

Applying the privacy principles to cloud computing

Contracted service provider requirements

In some circumstances an agency will have to take reasonable steps to make a contracted service provider subject to the privacy principles in the same way that the agency is. This obligation generally arises when, as part of the service agreement,

---

1 In this Guideline references to an “agency” include Ministers and bound contracted service providers, unless otherwise specified.
personal information will travel between the agency and the contractor. An agency planning to move to a cloud-based service may need to negotiate an alternative or additions to the cloud provider's standard terms and conditions in order to meet this obligation. A failure to take these reasonable steps may make the agency liable for any privacy breach by the cloud provider.

**Transfer out of Australia rules**

The IP Act only permits personal information to be sent out of Australia in the circumstances set out in section 33. Agencies should check where a cloud provider operates from, even when dealing with an Australian company. If the provider, or the hardware used by that provider, is not located in Australia, agencies will need to ensure they comply with section 33 for any personal information sent to the cloud.

When moving to cloud services, agencies may be able to comply with the obligations in section 33, at least in part, by entering into a contract with the cloud services vendor which provides for the same level of privacy protections as are in the IP Act.\(^2\)

**Protection and security (IPP 4, NPP 4)**

Agencies are required to ensure that personal information is properly protected against loss and unauthorised access, use and disclosure. This means agencies will have to consider the security a cloud provider will apply to their information and whether this complies with the privacy principles. Agencies might also wish to consider whether the agreement obliges the provider to notify the agency if security is breached.

**Access and amendment rights (IPP 6 and 7, NPP 6 and 7)**

The privacy principles give individuals the right to seek access to their personal information, and to have it amended where it is inaccurate; these rights reflect the access and amendment rights in chapter 3 of the IP Act. Agency information which is stored in the cloud is subject to these rights in the same way as information stored in a filing cabinet; agencies will need to ensure that information stored in the cloud is not overlooked when searches are being undertaken to locate information relevant to an access or amendment application.

**Use and disclosure (IPP 10 and IPP 11, NPP 2)**

If an agency's agreement with a cloud provider allows the agency to retain control over and sole access to its information, then the transfer of information from the agency computer to the cloud provider's computer will be a ‘use' and not a 'disclosure'.\(^3\)

---

\(^2\) See section 33(d)(i). If relying on section 33(d), agencies must ensure that at least two of the required elements are met.

\(^3\) See section 23 of the IP Act.
However, if the agreement does not allow the agency to retain control over the information, or it allows the cloud provider to access the information—for example, it permits scanning of the information for marketing purposes—this will be a disclosure. Disclosure is only permitted in the circumstances set out in the privacy principles. Agencies should identify any terms in the cloud agreement which give the provider the right to access agency data and consider whether they fall within the disclosures permitted under the privacy principles.

Other issues

Mandatory notification of a security breach

The nature of cloud computing means that an agency's information will be held by another entity and the agency has to rely on the cloud provider to tell them if something happens which affects the security of its information. Agencies should consider including a mandatory breach notification clause in all agreements with cloud providers. This will oblige the cloud provider to tell the agency if there has been an incident which may have impacted on the security of its data; this, in turn, will let the agency take steps to minimise the negative impacts of such a breach.

Lawful access in other countries

If a cloud provider or its hardware is located in a country outside of Australia, an agency's information may be subject to the laws of that country. For example, information stored on a server physically located in the United States of America may be subject to the Patriot Act, which allows broad access by the government to data located in the country. An agency planning to use a cloud provider located in another country should consider the impact of any such laws on their information.

Further reading


---

4 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001.
For additional information and assistance please refer to the OIC’s disclosure checklist, contracted service provider, overseas transfer guidelines, or contact the Enquiries Service 07 3234 7373 or email enquiries@oic.qld.gov.au.

This guide is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au

Published 1 December 2010 and Last Updated 11 November 2020

Changes to legislation after the update date are not included in this document