



Privacy and Cloud Computing for Australian Government Agencies

Better Practice Guide

Introduction

Despite common perceptions, cloud computing has the potential to enhance privacy safeguards used to protect personal information held by Government agencies.

This Better Practice Guide has been developed to assist agencies subject to the *Financial Management and Accountability Act 1997* (FMA Act) better understand how to comply with privacy laws and regulations when choosing cloud based services.

Irrespective of choosing traditional methods of provisioning ICT requirements or cloud computing services, agencies need to be aware of their privacy and security obligations, conduct a risk-based analysis of their information, and ensure that the contractual arrangements they enter into with ICT providers adequately address their privacy obligations.

It is important to note that the *Privacy Act 1988* (Privacy Act) does not prohibit the use of cloud computing and an agency, having conducted appropriate due diligence, may contract for cloud computing services and comply with its Privacy Act obligations, as with current ICT contractual practice.

Agencies are advised to conduct a risk-based analysis of their information, including a Privacy Impact Assessment, to determine the most appropriate ICT environment to deploy to support the classification of their information and business requirements.

Where an agency cannot adequately address its privacy obligations, it will not be appropriate to transfer that information into a public cloud environment.

Why is the guide needed?

Cloud computing poses a range of privacy issues which an agency will need to address and mitigate with appropriate legal, contractual and operational procedures as the cloud service provider assumes responsibility for hosting the information.

This document contains a non-exhaustive list of issues related to privacy and information security that an agency should investigate when considering cloud based services to ensure that the contract they agree with cloud service providers adequately addresses the applicable privacy obligations.

This document does not advocate or prohibit the use of cloud computing services, favour the private over public cloud model, favour on-shore over off-shore cloud service providers nor

does it discourage agencies from conducting appropriate due diligence as would be expected in any government procurement activity.

Agencies are reminded of their responsibility to comply with Commonwealth Procurement Guidelines and to read this document in conjunction with other Australian Government cloud computing related guidance, including:

- Defence Signals Directorate's [Cloud Computing Security Considerations Paper](#)¹;
- National Archives of Australia's [Records Management and the Cloud](#)²;
- Australian Government Solicitor's [Negotiating the Cloud – Legal Issues in Cloud Computing Agreements](#); and
- Department of Finance and Deregulation's [Financial Considerations for Government Use of Cloud Computing](#).

Key Resources

Privacy Act 1988 (Cth)

The Privacy Act and the eleven Information Privacy Principles (IPPs) set out in section 14 of the Privacy Act regulate how Commonwealth agencies collect, use, and disclose the personal information of individuals.

Personal information is information or an opinion about an individual whose identity is apparent, or could reasonably be ascertained, from the information or opinion.

Section 95B

Agencies should be aware that section 95B of the Privacy Act requires agencies to take contractual measures to ensure that contracted services providers do not do anything that would breach the IPPs.

Agencies that contract with cloud service providers will need to ensure that the contract stipulates personal information will be adequately protected by having the cloud service provider acknowledge in the contract that it will comply with the IPPs.

The obligations under section 95B of the Privacy Act apply regardless of whether the contractor is in Australia or off-shore.

When contracting off-shore, agencies need to make sure that they are still able to enforce the provisions of the contract. More information about privacy obligations for Commonwealth contracts can be found on the OAIC's website at www.oaic.gov.au.

Privacy Impact Assessment

The Office of the Australian Information Commissioner (OAIC) recommends that agencies carefully assess potential privacy impacts by undertaking a Privacy Impact Assessment (PIA) prior to making a decision about the use of cloud computing.

Agencies should refer to the OAIC's [Privacy Impact Assessment Guide](#)³ for further information.

¹ <http://www.dsd.gov.au/infosec/cloudsecurity.htm>

² <http://www.naa.gov.au/records-management/publications/cloud-checklist.aspx>

³ http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html

Key Issues

Notification

When an agency collects personal information, **IPP 2 - Solicitation of personal information from individual** requires the agency to advise the individual concerned whether the information is likely to be disclosed to any other entity.

Disclosure of personal information

IPP 11 - limits on disclosure of personal information controls the circumstances in which an agency can disclose personal information. If an agency shares personal information with a contracted cloud service provider, this may be considered a 'use' rather than a 'disclosure' under the Privacy Act, depending on the degree of control the agency retains over the personal information.

An agency that gives up its control over the personal information to the outsider is treated as *disclosing* that information. An agency that maintains control over the personal information is treated as *using* that information.

The extent of control necessary to qualify the sharing of personal information with a contracted service provider as a use as opposed to a disclosure will depend on the circumstances. Some indicators that an agency maintains control over personal information shared with a contracted service provider include:

- the agency gives the personal information to the outsider to use for a limited purpose that assists or benefits the agency. In the case of a cloud service provider, such use would ordinarily be use for the purpose of providing the relevant services to the agency (including trouble-shooting or problem-fixing);
- an agreement between the agency and outsider binds the outsider not to use or disclose the personal information except for the limited purpose or to its sub-contractors (who also agree to the same obligations); and
- an agreement between the agency and the outsider gives the agency the right to access, change or retrieve the personal information.

More information on use and disclosure of personal information can be found in the OAIC's [Plain English Guidelines to Information Privacy Principles 8-11](#)⁴.

Agencies should consider whether the engagement of a cloud service provider that may store or process personal information off-shore can allow agencies to retain the degree of control necessary for the sharing of personal information to constitute a use, rather than a disclosure.

In most cases, the information can still be sufficiently within the control of the agency for the sharing to constitute a use even if it is hosted outside of Australia, provided that effective contractual protections are put in place by the agency, such as ensuring the agency has the right under the contract and in practice to access or recover the information at all times.

Storage and security of personal information

When an Australian Government agency determines to use cloud based services to host its information, irrespective of the cloud service provider being located on-shore or off-shore, the cloud service provider will need to ensure it complies with **IPP 4 - Storage and security of personal information**.

⁴ <http://www.privacy.gov.au/materials/types/download/8700/6538>

IPP 4 requires that agencies ensure that personal information that they hold is protected, by such security safeguards, as it is reasonable in the circumstances to take, against misuse or loss, and unauthorised access, use, modification or disclosure.

This includes being able to control security measures. When the provider is located off-shore, satisfying IPP 4 may be more difficult. By using a cloud service, an agency is relinquishing some degree of control over its data, but not its responsibilities to ensure compliance with the Privacy Act.

Agencies are directed to the DSD interim guidance on *Cloud Computing Security Considerations* for further information regarding information security.

The most straight forward way to ensure the cloud service provider acknowledges that it will comply with the IPPs is by having the cloud service provider acknowledge in the contract that it will comply with the applicable IPPs.

Data segregation

Where the information of multiple agencies is being hosted in a single cloud (a community cloud), there should be adequate separation and segregation between the various datasets to prevent any inadvertent disclosure.

Data segregation⁵ should also occur where a government department is sharing a cloud server with, for example, private sector organisations. This is also relevant where a government department has multiple business units that may require data segregation – for example, some larger departments have distinct, separate business units which hold information that other units should not need to access.

Many cloud service providers will have such segregation built into their cloud offerings. However, where there are specific concerns around separation and segregation, an agency should obtain all pertinent technical information from the service provider to ensure the proposed solution provides the required level of data segregation.

Where required, additional processes or arrangements for data segregation and security will need to be agreed with the cloud service provider. This may include a data classification system whereby only some information – such as non-personal or de-identified information – is stored in the cloud.

Data destruction

The IPPs do not contain an express obligation for agencies to destroy or permanently de-identify personal information that is no longer required, although this requirement is likely to be extended to agencies by the reforms to the Privacy Act (see further below). In any case, destruction or de-identification of information will usually be a ‘reasonable step’ to prevent the loss or misuse of that information (as required by IPP 4).

Accordingly, agencies should carefully consider retention practices, subject to record keeping requirements such as those contained in the *Archives Act 1983* (Cth) (including their Records Disposal Authorities) or other legislation.

Agencies should ensure that information in the cloud can be permanently deleted when it is no longer required or at the end of the contract. Again, this can be achieved by having the cloud service provider acknowledge in the contract that it will comply with the applicable IPPs.

⁵ Data segregation can be physical or virtual (also known as data partitioning).

Note that obligations relating to the preservation of public records will still apply. (See National Australia Archives *Records Management and the Cloud*)

Transborder data flows

Agencies should be aware that, when contracting off-shore cloud computing services, information may be processed or stored in jurisdictions with privacy and information protection laws significantly different from those in Australia.

This can make enforcement of contractual measures under s 95B of the Privacy Act, and other contractual obligations, such as those relating to data breaches, challenging. To mitigate this risk, agencies are advised to have the cloud service provider acknowledge in the contract that it will comply with the Privacy Act.

Agencies should note it may also be possible for foreign governments to access information held in their jurisdiction or to access information held in Australia by any company with a presence in their jurisdiction.

For instance, the USA PATRIOT Act 2001 contains provisions allowing the US Government to access information in specified circumstances, (i.e. cases involving suspected terrorism or threats to national security) irrespective of the geographical location and, without necessarily advising the agency.

Agencies are reminded that current Defence Signals Directorate advice requires agencies to consider the risks including sensitivity, privacy and security in providing information to any third party.

Risks arising from foreign legislation, including the Patriot Act, should be considered in conjunction with all Australian legislative requirements.

Contract management

Agencies may also wish to consider including requirements in contracts that would enhance control over personal information. While the requirements set out below are not mandated by the Privacy Act or the IPPs, an agency may consider circumstances exist which justify a greater level of protection. Issues to consider and be negotiated with providers include:

- where information will be physically located and whether the physical location of the information is of such significance to the agency that it should seek from the provider specific stipulations as to information location and make the relocating of information conditional upon an agency's permission.
- the legislative environment in those locations if the applicable governing law is the law of a foreign country;
- what type of security measures will be used for storage and what (if any) encryption is used during transmission;
- who will be able to access the information;
- whether access to information can be audited or third party audit findings can be shared;
- how backup copies of the information are protected;
- whether a requirement for information breach notification should be included in the contract;
- whether information no longer needed can be permanently deleted at the end of the contract, and

- who has control of the information at the end of the contract?

As noted above, while such requirements are not explicitly required by the Privacy Act, they can demonstrate a commitment to achieving best privacy practice. It should be noted that requirements outside of standard cloud service provider offerings may increase costs.

It is important that the contract and the cloud services be reviewed with the provider over the life of the contract, and in particular following any change to privacy laws, to ensure that information security measures are kept up-to-date.

Privacy Act reform: The Australian Privacy Principles

The Government is currently in the process of reforming the Privacy Act. The reforms include the introduction of a set of unified privacy principles known as the Australian Privacy Principles (APPs), which will apply to both government agencies and private sector organisations.

In July 2010, the Government released an *exposure draft of the APPs*.⁶ The Senate Finance and Public Administration Committee released its report on the exposure draft legislation in June 2011. At the time of writing, the Government had not yet responded to the report.

It is recommended that agencies monitor developments in the privacy law reform process, as these may have significant implications for agencies contemplating the use of off-shore cloud service providers.

Agencies should have processes in place to ensure that cloud service providers are informed of and educated about any Privacy Act or *Freedom of Information Act 1982* (FOI Act) amendments and recognise their obligations under any amended legislation.

Acknowledgements

The Department of Finance and Deregulation wishes to thank the staff of the Office of the Australian Information Commissioner, members from the Cloud Information Community and the considerable contribution from members of the Australian Information Industry Association for the collation and review of the material in this guide.

⁶ http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/

Summary of Checkpoints

| | |
|---|--------------------------|
| <p>1. Has your agency established a policy or procedure for deciding when it will be appropriate to use cloud computing services?</p> <p>Does the policy or procedure address the following?</p> <ul style="list-style-type: none"> • will the proposal involve the storage or processing of personal information? • if so, is an assessment of the ability of a cloud solution to provide adequate protection to the personal information required? • if sensitive personal information is involved, what extra measures might be required? • what type of cloud service provider will be appropriate? (e.g. private, public or community) | <input type="checkbox"/> |
| <p>2. Has your agency decided what it will use cloud service infrastructure for?</p> <ul style="list-style-type: none"> • just storing • just processing • both storing and processing | <input type="checkbox"/> |
| <p>3. Has your agency developed a contract with the cloud service provider that is consistent with s95B of the Privacy Act?</p> <p>How will your agency ensure that the contract's requirements are being met?</p> | <input type="checkbox"/> |
| <p>4. Has your agency considered what specific terms should be included in the contract to complement the general requirement under s 95B to adhere to the IPPs?</p> <p>Some specific matters that could be addressed in the contract include requirements relating to:</p> <ul style="list-style-type: none"> • data breach notification • the location of information • access to information by agency staff • audits | <input type="checkbox"/> |
| <p>5. If personal information is to be disclosed to a cloud service provider, has your agency determined how that disclosure will be authorised?</p> <ul style="list-style-type: none"> • express permission from individuals • individuals are notified in privacy notice/terms and conditions • by legislative provisions | <input type="checkbox"/> |
| <p>6. If you are intending to use an off-shore cloud service provider, do you know where their head office is located?</p> | <input type="checkbox"/> |

| | | |
|-----|--|--------------------------|
| | What are the privacy implications? | |
| 7. | Does your agency know where the data will be stored; keeping in mind the possibility it may be across different countries or continents? What are the Privacy implications? | <input type="checkbox"/> |
| 8. | Keeping in mind privacy law reform, has your agency determined that there is data protection or privacy legislation in place in relevant foreign jurisdictions that, at a minimum, meets the requirements in the Privacy Act? Is the relevant law enforceable? | <input type="checkbox"/> |
| 9. | Has your agency determined how the personal information will be kept separate from other organisations' data housed in the cloud service provider's infrastructure? | <input type="checkbox"/> |
| 10. | Has your agency determined how employees of the cloud service provider will be prevented from unauthorised access to the data? Has your agency decided how it will control a cloud service provider passing personal information onto unauthorised third party organisations or using it for purposes other than those it was originally collected for? | <input type="checkbox"/> |
| 11. | Has your agency determined how it will monitor the cloud service provider's use and management of the agency's information? | <input type="checkbox"/> |
| 12. | Has your agency determined the controls (for example, encryption) that will be in place to ensure the security of personal information as it travels between here and possible overseas cloud data storage location? | <input type="checkbox"/> |
| 13. | If an Australian citizen requests access or alteration to their personal information, has your agency put in place appropriate controls so that all copies can be retrieved and amended easily? Has your agency put in place arrangements to ensure that where an individual requests an amendment to their personal information and this request is not agreed to, it will be possible to attach a statement provided by the individual regarding the requested amendment to the record? | <input type="checkbox"/> |
| 14. | Has your agency ensured that the cloud service provider will hold the personal information only as long as your agency needs it? Has your agency specified how the cloud service provider will manage their backup regime? Has your agency specified how personal information that is no longer needed is to be destroyed or de-identified? | <input type="checkbox"/> |
| 15. | Has your agency determined what happens at the conclusion of the contract with the cloud service provider? Will information be able to be retrieved or destroyed (including all backups where appropriate) in compliance with the Privacy Act and associated legislation? | <input type="checkbox"/> |

© Commonwealth of Australia 2012

Apart from any use permitted under the Copyright Act 1968, and the rights explicitly granted below, all rights are reserved.

You are free to copy, distribute and transmit the work as long as you attribute the authors. You may not use this work for commercial purposes. You may not alter, transform, or build upon this work.

Except where otherwise noted, any reference to, reuse or distribution of all or part of this report must include the following attribution:

Privacy and Cloud Computing for Australian Government Agencies, Copyright Australian Government 2012.



Licence: This document is licensed under a Creative Commons Attribution Non-Commercial No Derivs 3.0 licence.

To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/legalcode>.

Any of the above conditions can be waived if you get our permission. Requests for permission should be addressed in the first instance to aga@finance.gov.au