Government of South Australia

Privacy Committee
Of South Australia

Privacy & Cloud Computing Guideline

Publication

October 2013

Version **1.2**

Executive Officer
Privacy Committee of South Australia
c/o State Records of South Australia
GPO Box 464
ADELAIDE SA 5001
Phone (08) 8204 8786
privacy@sa.gov.au

Table of Contents

Introduction

This Guideline has been developed to assist agencies subject to the South Australian Government's Information Privacy Principles (IPPs) Instruction, issued as Premier and Cabinet Circular 12 - Cabinet Administrative Instruction No.1 of 1989 (IPPs Instruction or IPPs), better understand how to comply with the IPPs when utilising cloud based technologies.

Irrespective of choosing cloud computing services or other traditional methods for storing or transmitting data within or outside of government, agencies remain accountable for how that data is protected. Contract provisions provide limited protection when dealing with a global and complex cloud environment. Agencies should ensure that they are aware of their privacy and security obligations and conduct a Privacy Impact Assessment before entering into a contractual arrangement with an Information and Communications Technology (ICT) provider.

Why is this Guideline needed?

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

This Guideline contains a non-exhaustive list of issues related to privacy and information security that an agency should consider and further investigate when contemplating cloud computing to ensure that the contract they enter into with a cloud service provider adequately addresses the applicable privacy obligations.

This Guideline 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 South Australian Government procurement obligations and to read this document in conjunction with other South Australian Government privacy, cloud computing, and contractual guidance documents, including those identified at the end of this document.

What are the Information Privacy Principles?

South Australian Government agencies are required to comply with ten privacy principles as described in the IPPs Instruction. In addition, employees of the Department for Health and Ageing and the Department for Communities and Social Inclusion are required to comply with the *Code of Fair Information Practice*. Contracted service providers providing a service on behalf of government are also required to comply with the IPPs when handling personal information.

The IPPs exist to keep personal information safe from inappropriate collection, use or disclosure by State Government agencies while still allowing information to be shared where appropriate. They recognise the need to balance personal privacy with the broader public interest.

For further information, please refer to the *Short Guide to the Information Privacy Principles.*

What is Personal Information?

Personal information means *'information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained*[1] *'.* A natural person in this context is a living human being. Determining whether a person's identity is apparent or can be reasonably ascertained depends on the context of the information and the circumstances of the particular situation.

Personal information can include combinations of name, address, date of birth, financial or health status, ethnicity, gender, religion, witness statements, alleged behaviours and licensing details. It may also include photographs or video footage of individuals/data subjects.

What is Cloud Computing?

Cloud computing is not a new concept; it is already a major part of many people's lives. It is an "ICT sourcing and delivery model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[2]".

Translated to layman's terms, this means internet based services provided to organisations wishing to procure computing resources from external suppliers rather than establishing and maintaining systems, platforms and infrastructure 'in-house'. What is fundamentally different about cloud is that in many cases it is no longer government which owns the hardware, software and networks through which information is transmitted and stored. These can effectively be anywhere in the world and may in fact be split across many data centres in many differing countries. Examples of cloud computing include Google Maps, Apple iTunes, Amazon Web Services and Microsoft's Hotmail.

[1] Clause 3(1) of Cabinet Administrative Instruction No.1 of 1989 (Information Privacy Principles Instruction), Government of South Australia.

[2] The NIST Definition of Cloud Computing (SP 800-145), National Institute of Standards and Technology, US Department of Commerce, September 2011, http://csrc.nist.gov/publications/PubsSPs.html#800-145.

Applying the IPPs to Cloud Technology

The IPPs exist to ensure State Government agencies keep personal information safe from inappropriate collection, use and disclosure.

If the data to be stored in the cloud includes personal information, the Principal Officer[3] of an agency has a responsibility to ensure that the IPPs are observed within the agency, and that privacy obligations are formalised within a contract with the third party providing a service on behalf of the agency. The Principal Officer remains accountable for the information, whether it is stored in the agency or through a cloud service provider.

Privacy Risks

Cloud computing can trigger a number of privacy risks, such as the lack of control over personal information and lack of transparency about how, where and by whom data is being processed. By placing personal information into the cloud, agencies may no longer be in exclusive control of this data. When an agency utilises a cloud service provider the information they transfer to that provider may be subject to the data privacy laws of more than one country. Insufficient assessment about a cloud service provider's location, legislative environment, operations and lack of awareness of the potential threats and risks, and subsequent inability to mitigate those risks, poses a risk to agencies and data subjects.

If an agency is to consider de-identifying personal information for storage in the cloud the resources required to de-identify the personal information should be considered. De-identification of personal information can require substantial work on the part of the agency, which is often not properly considered. With increasing sophistication of data mashing and data matching, which are the processes of weaving together structured data from different sources, there is a risk of re-identification of personal information.

To assess and manage these risks, agencies need to understand how they organize, classify and manage their information, which then provides a foundation for assessing potential cloud service providers. Cloud computing can be used in a way that does not compromise the privacy of personal information provided privacy risks are recognised at the foundation of the project or initiative and embedded into contracts.

Agencies may wish to consider including requirements in contracts that will enhance control over personal information. While the considerations below are not mandated by the IPPs, agencies could demonstrate a commitment to best privacy practice by considering and negotiating the following with the service provider:

- If the service provider is owned or controlled by a foreign company, define the level of control the foreign company will have over data handled by the service provider.

[3] See clause 3(1) of Cabinet Administrative Instruction No 1 of 1989 (Information Privacy Principles Instruction), Government of South Australia, for the definition of Principal Officer.

- Where information will be physically located. If the proposed location presents significant risks, the agency should consider seeking assurances from the provider that the information will only be stored in low risk locations and that the information will only be relocated with the agency's permission.

- The legislative environment in those locations if that of a foreign country.

- What type of security measures will be used for storage and what (if any) encryption will be used during transmission when the data is most vulnerable.

- Who will be able to access the information, and how unauthorised access by system administrators or staff of the cloud service provider will be prevented.

- Whether the cloud service provider is willing to undergo on-demand or periodic audits by the agency or a nominated third party, in relation to information security and access arrangements.

- Whether back-up copies of the information are made, how those copies are to be protected and how long they are kept.

- Requirements to notify the agency of any data breaches, methods of notification and responses to such breaches.

- At the conclusion of the contract, how and in what format information required to be retained by the agency will be returned to the agency in accordance with the *State Records Act 1997*.

- At the conclusion of the contract, how any information which is no longer required will be destroyed by the service provider.

Prior to making a decision about the use of cloud computing, agencies are advised to conduct a Privacy Impact Assessment to identify the potential privacy impacts of using cloud computing.

The Privacy Committee recommends that agencies follow the Office of the Australian Information Commissioner's Privacy Impact Assessment Guideline, which can be accessed at http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html.

A Checklist of issues for agencies to take into account when considering using a cloud solution to handle personal information can be found at Appendix A.

Where the risks cannot be quantified due to insufficient information, the risks are too complex to be calculated, or an agency cannot adequately satisfy its privacy obligations, it is considered not appropriate to enter into a cloud arrangement.

Contract Management

If, after undertaking a Privacy Impact Assessment, agencies decide to utilise cloud based technologies, they must comply with clause 5 of the IPPs – Access to Records of Personal Information. Clause 5 was amended in 2009 to recognise that agencies need to disclose personal information to contracted service providers delivering services on behalf of government and to ensure that personal information handled by the service provider is managed in line with the IPPs. The IPPs include provisions to ensure both parties are accountable for the protection of the personal information they handle, in that the IPPs require personal information handled by contracted service providers to be treated in the same way that it would be if the agency were delivering the service themselves.

Any contracts that involve the handling of personal information must include obligations on the service provider to ensure the personal information is treated in line with the IPPs. Model Terms and Conditions were developed to assist agencies to meet their obligations under the IPPs.

The contract for cloud services should be reviewed with the provider over the life of the contract, and if possible updated to ensure it complies with any change to privacy or security laws or practice.

For more information about contracting and the IPPs, please refer to the Contracting and the Information Privacy Principles information sheet and Contracting and Official Records Standard and Guideline which can be found on the State Records website www.government.archives.sa.gov.au.

For information about the development of contractual and operational arrangements, agencies should refer to standard State Procurement Board[4] and/or Crown Solicitor's Office[5] contracts, and may also wish to review current and developing international standards and protocols[6].

Transborder Data Flows

Transborder data flow refers to the flow of data from an entity in one jurisdiction to an entity in another jurisdiction. Agencies should be aware that, when contracting off-shore cloud computing services, information may be processed or stored in jurisdictions with privacy and information laws significantly different to those in Australia. This can make enforcement of contractual obligations, such as those relating to data breaches, challenging. To mitigate this risk, agencies must include conditions in the contract in accordance with clause 5(A) of the IPPs to ensure that the cloud service provider will comply with the South Australian Government's IPPs.

[4] For further information see http://www.spb.sa.gov.au/site/home.aspx.

[5] For further information see http://www.agd.sa.gov.au/government/about-us/department/crown-solicitors-office.

[6] For example, the International Organization for Standardization's ISO/IEC 27000-2701, see http://www.iso.org/iso/home/standards.htm.

Agencies should also note that it may 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. Some legislation of international jurisdictions contain provisions allowing that government to access information in specified circumstances, such as cases involving suspected terrorism or threats to national security, irrespective of the geographical location and without necessarily advising the South Australian Government. Risks arising from foreign legislation should be considered in conjunction with all Australian legislative requirements.

Information Storage & Security

When an agency determines to use cloud computing to host its information, the cloud service provider will need to ensure it complies with IPP 4 – Storage of Personal Information. IPP 4 requires that agencies *'take such steps as are, in the circumstances, reasonable to ensure that personal information in its possession or under its control is securely stored and is not misused'.*

When a service provider is located off-shore, satisfying IPP 4 may be more difficult. While using a cloud computing service may reduce, to some degree, control over its data, it does not relinquish or diminish an agency's responsibility to ensure compliance with the IPPs. Imposing contractual obligations on the cloud service provider in regard to storage and security will ensure compliance with IPP 4.

Agencies should have policies concerning the storage and classification of personal information in accordance with the requirements of the Government's Protective Security Management Framework, the Information Security Management Framework, and Records Management Standards and Guidelines issued under the *State Records Act 1997*. If an agency is unclear about their security policies or procedures they should contact their Agency Security Advisor.

Data Segregation

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

Data segregation may also be necessary where a government department is sharing a cloud computing server with, for example, private sector organisations, or where a government department has multiple business units and one unit holds information that other units do not have a right of access to.

Many cloud service providers will have such segregation built into their cloud computing solutions. However, where there are requirements for segregation of data, 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 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.

Records Management

Some of the advice provided to ensure compliance with the IPPs will also help to ensure that good records management principles are followed when using cloud computing. Safeguards against unauthorised access and misuse of information are benchmarks of adequate records management.

In addition to undertaking a Privacy Impact Assessment, an agency must also comply with the *State Records Act 1997* and consider risks such as:

- unauthorised access to records
- inadequate creation / retention of metadata
- loss of access to records
- records destruction or loss
- damage to the evidential value of records – records must be authentic and reliable.

The service provider should be able to provide assurances that:

- comprehensive audit trails and descriptions of management processes are created and retained to verify the authenticity and reliability of the records
- sufficient metadata fields can be provided to satisfy recordkeeping and business requirements (as described in the South Australian Recordkeeping Metadata Standard published on www.government.archives.sa.gov.au)
- records can be destroyed at the agency's direction and the service provider issue a certificate of destruction
- procedures for third party access to the records, for example from local security agencies, will be managed
- procedures for backup and restoration of records are in place in the event of loss or damage.

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. Destruction or permanent de-identification of information will usually be a 'reasonable step' to prevent the misuse of that information (under IPP 4).

Accordingly, agencies should carefully consider retention practices, subject to record keeping requirements such as those contained in the *State Records Act 1997*. Specifically, the process by which official records of government are either destroyed, retained or transferred between agencies.

Agencies should ensure that information stored in the cloud can be permanently deleted when it is no longer required or at the end of the contract and that no copies will be retained by the service provider.

Other Relevant Documents

Short Guide to the Information Privacy Principles

Records Management and Cloud Computing

Contracting and the Information Privacy Principles Information Sheet

Contracting and Official Records Standard

Contracting and Official Records Guideline

Model Terms and Conditions – IPPs and Records Management

ISMF Guideline 8 – Cloud Computing

TSSSC Overview and Considerations for Cloud Computing

Acknowledgments

The Privacy Committee of South Australia acknowledges the informative work undertaken by the Australian Government Information Management Office, Department of Finance and Deregulation, Office of the Victorian Privacy Commissioner, and the Office of the Information Commissioner Queensland. This Guideline builds on the guidance material produced by those offices.

Appendix A - Checklist

The issues an agency should take into account when considering using a cloud solution to handle personal information include:

1.	Has your agency established a policy or procedure for deciding when it will be appropriate to use cloud computing services? Does the policy or procedure address the following? • 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, such as that which relates to child protection or is classified sensitive: commercial, what extra measures might be required? • what type of cloud service provider will be appropriate? (eg private, public, community, hybrid[7])	☐
2.	Has your agency decided what it will use cloud service infrastructure for? • storage of information • processing of information • both storing and processing information	☐
3.	Has your agency developed a contract with a cloud service provider that is consistent with clause 5 of the IPPs Instruction and the Contracting and Official Records Standard and Guideline? (refer to the Contracting and the Information Privacy Principles Information Sheet for further information) How will your agency ensure that the contract's requirements are being met?	☐
4.	Has your agency considered what specific terms should be included in the contract to comply with the above requirements? Some specific matters that could be addressed in the contract include requirements relating to: • data breach notification • the location of information • access to information by agency staff • the right of the agency to audit the service provider	☐

[7] For definitions, see section 9 of the TSSSC Overview and Considerations for Cloud Computing at http://www.sage.sa.gov.au/display/ICTPolicy/Cloud+Computing+in+SA+Government.

	• retrieval or destruction of the information at the conclusion of the contract	
5.	If personal information is to be disclosed to a cloud service provider, and clause 5 of the IPPs Instruction has not been initiated, has your agency determined how that disclosure will consequently be authorised? • express permission from individuals • individuals are notified in privacy notice / terms and conditions • by legislative provisions	☐
6.	If your agency is intending to use an off-shore cloud service provider, do you know where their head office is located? What are the privacy implications?	☐
7.	Does your agency know where the information will be stored; keeping in mind the possibility that it may be held in a number of different countries or continents? What are the privacy implications?	☐
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 IPPs? Is the relevant law enforceable in that jurisdiction?	☐
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?	☐
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?	☐
11.	Has your agency determined how it will monitor the cloud service provider's use and management of the agency's information?	☐
12.	Has your agency determined the controls (for example, encryption) that will be in place to ensure the security of personal information as it is transferred between the agency and the service provider, bearing in mind that the provider's data store may reside outside of Australia?	☐
13.	Has your agency ensured it has retained backup copies of the information within the agency or the South Australian Government ICT environment (in case of insolvency or prolonged outage to the cloud service)?	☐

14.	If a member of the public requests access to or alteration of 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, a notation can be added to the record, in accordance with section 37 of the *Freedom of Information Act 1991*?	☐
15.	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?	☐
16.	Has your agency determined what happens at the conclusion of the contract with the cloud service provider? Will the information be able to be retrieved or destroyed (including all backups where appropriate) in compliance with the IPPs and associated legislation?	☐