Information Commissioner
NORTHERN TERRITORY

CLOUD COMPUTING

&

PRIVACY PRINCIPLES GUIDELINES

May 2017
Version 1.0

The Office of the Information Commissioner expresses thanks to the Office of the Information Commissioner Queensland for their assistance in preparing this Guideline

Contents

Overview

The *Information Act* (the 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 Northern Territory public sector organisations (PSOs)[1].

Personal Information

Personal information is defined in Part 1, section 4A of the 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.

Specifically, the section states that Government information that discloses a person's identify or from which a person's identity is reasonably ascertainable is ***personal information***.

However, the government information is not ***personal information*** to the extent that:

(a) the person's identity is disclosed only in the context of having acted in an official capacity for a public sector organisation; and
(b) the government information discloses no other personal information about the person.

What are the privacy principles?

The Information Privacy Principles (IPPs) are a specific set of obligations set out in Schedule 2 of the Act. They are legislated responsibilities of Territory public sector organisations (PSOs) for the handling and use of information and include:

• Collection (IPP 1)	• Access and Correction (IPP 6)
• Use and Disclosure (IPP 2)	• Identifiers (IPP 7)
• Data Quality (IPP 3)	• Anonymity (IPP 8)
• Data Security (IPP 4)	• Transborder Data Flows (IPP 9)
• Openness (IPP 5)	• Sensitive Information (IPP 10)

What is cloud computing?

Cloud computing is not a new concept. Webmail services such as Hotmail for example, have been around since 1997. The phrase 'cloud computing' is simply a term for moving functions from a computer and an agency-owned server to an online environment. Employees accessing word processing programs through a webpage interface instead of the programs menu on their computer is an example.

Computer 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.

[1] In this Guidelines references to a "public sector organisation" refers to section 5 of the Act and includes entities such as an Agency, Government Business Division, local government council, the Police Force of the Northern Territory and bound contracted service providers unless otherwise indicated.

Applying the privacy principles to cloud computing

Contracted service provider requirements

In some circumstances a PSO 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, personal information will travel between the agency and contractor. A PSO planning to move to a cloud-based service may need to negotiate an alternative or additions to the cloud provider's service contract or standard terms and conditions in order to meet this obligation. A failure to take these reasonable steps may make the agency liable for any breach of privacy by the cloud provider.

Transfer Interstate or out of Australia (IPP 9)

The *Information Act* only allows personal information to be sent out of the Territory in the circumstances set out in IPP 9. PSOs 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 the Territory (or Australia), PSOs will need to ensure that they comply with IPP 9 for any personal information to be sent to the cloud.

When moving to cloud services, PSOs may be able to comply with obligations in IPP 9, 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 contained within the IPPs[2].

Data Quality and Security (IPP 3 & IPP 4)

PSOs must take reasonable steps to:

- ensure the personal information it collects, uses or discloses is accurate, complete and up to date;
- protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure;
- destroy or permanently de-identify personal information if it is no longer required for any purpose.

These aspects should be individually addressed by PSOs as well as covered off in contracts and agreements with cloud providers.

Access and correction rights (IPP 6)

The IPPs give individuals the right to seek access to their personal information, and have it corrected where it is inaccurate. PSO information which is stored in the cloud is subject to these rights in the same way as information stored in a filing cabinet. PSOs 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 correction application.

Use and disclosure (IPP 2)

If a PSO agreement with a cloud provider allows the PSO to retain control over and sole access to its information, then the transfer of information from the PSO's computer to the cloud provider's computer will be a 'use' and not a 'disclosure'.

[2] *Information Act*, Schedule 2, IPP 9, 9.1(b)

However, if the agreement does not allow the PSO 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. PSOs 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 permitted disclosures, for example – preventing, detecting, investigating , prosecuting or punishing an offence or a breach of a prescribed law.

Other issues

Mandatory notification of a security breach

The nature of cloud computing means that a PSO's information will be held by another entity and the PSO has to rely on the cloud provider to tell them if something happens which affects the security of its information. PSOs should consider including a mandatory breach notification clause in all agreements with cloud providers. This will oblige the cloud provider to tell the PSO if there has been an incident which may have impacted on the security of its data. This in turn will let the PSO 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 which is physically located in the United States of America may be subject to the USA's national security and intelligence legislation which may allow broad access by the government to data located in the country.

Summary of general elements to consider

Areas of risk management to address

- Front end
  - e.g. the IT architecture , administrative protocols, staff training, security and audit of the personal information within the PSO
- Back end
  - e.g. the IT architecture, administrative protocols, staff training, security and audit of the personal information when it is with the contract service provider
- the contractual provisions that require compliance with the IPPs and legally accept risk for data breaches

Other elements to consider

- PSO ability to audit the system
- whether PSO will be advised of a data breach by the provider
- the level of training of the provider
- the contractual arrangements for dealing with IPP 9 and risk management generally
- the type of training and guidance provided to PSO staff
- the type of training and guidance given to provider staff
- disposal issues – can PSO get their information back?
- who has access to the data and can they change it?

Department of Corporate and Information Services Requirements

The Department of Corporate and Information Services (DCIS) provides NT Government support in digital policy. The Digital Policy Unit develops and maintains ICT policies, standards, guidelines and procedures for government. PSOs should seek advice from this Unit when considering the procurement and implementation of cloud computing services. Risk factors should be accessed in relation to perceived benefits before a final business solution is agreed. Areas considered may include application design, architecture, business continuity, data location and retrieval, performance and conformance as well as security.

Legal Review and Advice – Solicitor for Northern Territory (SFNT)

As many of the unique risks associated with cloud computing are not addressed by standard government procurement processes, it is essential that PSOs obtain early legal advice from SFNT to assist in the procurement of their cloud service. The assistance that SFNT can provide includes incorporating the additional contractual clauses required, compliance with legislative requirements, addressing and mitigating legal risks, advice on ways to protect PSO rights, identification of any legal obligations the PSO is required to fulfil and any contract negotiations required.

General Cloud Based Questions / Key Elements to Address

Whenever a project is undertaken involving handling personal information (including engaging a contract service provider to handle personal information by or on behalf of government), the following should be considered:

- is the information travelling outside the NT? If so, it must be done in a manner compliant with IPP 9
    - where are the servers?
    - how will the information travel from the NT to those servers?
    - where will the information travel and who will handle it?
    - who provides IT support and where are they located? (diagram helps)
- how securely is the data stored?
    - what is the level of physical security?
    - what is the level of electronic security?
    - is there an audit log of access?
    - what is the level of granularity of control over user access and in the audit log?
    - are the people who are handling the data appropriately selected and trained?
- how sensitive is the data?
- how is the data being collected?
- have you considered the whole of life cycle of the information?
    - is permission being gained at the outset for all relevant purposes?
    - what is in place to ensure the information will be destroyed or de-identified when it is no longer needed?
- if a contract service provider is involved, has liability been shifted under s 149 of the *Information Act* (standard SFNT clause 11).

Further reading

- General Australian Government guidelines: http://www.asd.gov.au
- Cloud Computing Security Considerations (Department of Defence, Intelligence and Security): http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_Considerations.pdf
- A list of certified cloud services: http://www.asd.gov.au/infosec/irap/certified_clouds.htm
- The NT Information Privacy Principles: https://infocomm.nt.gov.au/privacy/information-privacy-principles
- Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing: http://www.worldprivacyforum.org/www/wprivacyforum/pdf/WPF_Cloud_Privacy_Report.pdf
- Commissioner for Privacy and Data Protection (Victoria): https://www.cpdp.vic.gov.au/images/content/pdf/Cloud_Computing_in_the_Victorian_Public_sector.pdf

For additional information and assistance,
please contact the Office of the Information Commissioner.

Information Commissioner
NORTHERN TERRITORY

1800 005 610 / 8999 1500
www.infocomm.nt.gov.au
infocomm@nt.gov.au

GPO Box 1344, Darwin NT 0801
Level 6, 22 Mitchell St, Darwin NT 0800