Office of the Information Commissioner
Queensland

IPOLA

# IPOLA GUIDELINE

# Applying the legislation – Information Privacy Act 2009

## Cloud computing and the privacy principles

**This guide does not reflect the current law.**

**It highlights important changes to the *Information Privacy Act 2009*.**

**This guide does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.**

### 1.0 Overview

The Queensland Privacy Principles (QPPs) in the *Information Privacy Act 2009* (Qld) (IP Act) set out the rules for how personal information must be collected, managed, used and disclosed by Queensland government agencies.[1]

### 2.0 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 or is reasonably identifiable. Information does not have to be true, written down, sensitive or 'important' to be personal information.

Refer to ***Key privacy concepts – personal and sensitive personal information*** for more information.

### 3.0 What is cloud computing?

The phrase 'cloud computing' is simply a shorthand term for moving functions from an agency-owned computer or server to a server owned by someone else which is accessed online. Microsoft 365, which allows programs such as Teams, Word and Excel to be used through a browser, is an example of cloud computing.

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.

[1] Agency includes a Minister, bound contracted service providers, and any other entity required to comply with the QPPs.

## 4.0 Applying the privacy principles to cloud computing

### *4.1 Contracted service provider requirements*

In some circumstances an agency will have to take reasonable steps to bind a contracted service provider to comply with the privacy principles as if they were an agency.[2] This obligation generally arises when, as part of the service agreement, 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.

Refer to ***Binding contractors to the IP Act*** (guideline under development) for more information.

### *4.2 Disclosure out of Australia rules*

In addition to the QPPs, agencies must comply with section 33, which only permits personal information to be disclosed out of Australia in specific circumstances. Disclosure outside of Australia requires more than the movement of personal information out of the country. The agency must cease to have control over the personal information once it has left Australia.[3]

Agencies should be aware of where a cloud provider operates and whether the terms and conditions of the agreement means the agency will cease to have control over information stored by the cloud provider. If the provider's servers are located overseas and the agency will lose control of information transferred to their servers, the agency must ensure that it complies with section 33.

Refer to the discussion below and ***Disclosing personal information out of Australia*** for more information.

### *4.3 Protection and security*

QPP 11 requires agencies to protect personal information against misuse, interference, loss, and unauthorised access, modification, or disclosure.

Agencies will need to consider the security a cloud provider will apply to their information and whether this complies with QPP 11. Agencies should also consider whether the agreement with any cloud computing service provider obliges, or should oblige, the provider to notify the agency if security is breached.

[2] Sections 34-37 of the IP Act.
[3] The concept of 'disclosure' is defined in section 23 of the IP Act.

### *4.4 Access and amendment rights*

QPPs 12 and 13 and the *Right to Information Act 2009* (Qld) give individuals the right to access and amend their personal information. Agency information which is stored with a cloud provider will ordinarily be subject to these rights.

Agencies must ensure information stored in the cloud is not overlooked when searches are being undertaken to locate information relevant to an access or amendment request.

### *4.5 Use or disclosure*

QPP 6 sets the rules for when personal information can be used or disclosed by an agency.

If an agency's agreement with a cloud provider allows the agency to retain control over its information, then the transfer of information from the agency computer to the cloud provider will be a use and not a disclosure.[4]

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 its own purposes, e.g., it permits scanning of the information for marketing purposes, transfer/storage of information will be a disclosure.

Agencies must ensure that the movement of personal information to a cloud provider complies with QPP 6.

Refer to ***Key privacy concepts – use and disclosure*** and ***QPP 6 - use or disclosure*** for more information.

### *4.6 Mandatory notification of a data breach*

Agencies have mandatory notification of data breach (**MND**) obligations under chapter 3A of the IP Act. These obligations apply to personal information contained in documents 'held' by an agency – information that is in the agency's possession, or under the agency's control. Personal information stored by an agency on a cloud computing service will generally remain under the agency's control, and will therefore be subject to MNDB obligations in the event of a breach. When agency information is stored on a cloud provider's systems, the agency is generally reliant on the cloud provider to advise the agency if there is of a security or data breach.

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 the agency's data. This will allow the agency to take steps to minimise the negative impacts of such a breach and meet the MNDB obligations.

For more information, see ***Mandatory Notification of Data Breach scheme***.

[4] Section 23 of the IP Act.

### *4.7 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,[5] 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.

## 5.0 Further reading

- QSA's Managing the Recordkeeping Risks Associated with Cloud Computing.
- World Privacy Forum: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing.
- Office of the Victorian Privacy Commissioner: Privacy and Cloud Computing: Cloud computing in the Victorian public sector.

**For additional IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au**

**For information and assistance on current legislation, please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au**

***Published August 2024 and Last Updated 22 August 2024***

[5] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (USA PATRIOT) Act of 2001.