Australian Government Solicitor the leading lawyers to government

AGS

Express law
fast track information for clients

12 July 2013

New Risk management guidelines for outsourced or offshore ICT arrangements

On 5 July 2013 the Attorney-General's Department published the *Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements* (Policy and Risk management guidelines).

The Policy explains that for certain types of data, additional controls on the storage and processing of Australian Government information in outsourced or offshore ICT arrangements are required. For example, where an agency is considering storage or processing of information defined as 'personal information' in the *Privacy Act 1988* in outsourced or offshore ICT arrangements, the agency is to seek agreement from its own Minister, and from the Attorney-General, the minister responsible for privacy as well as protective security in the Australian Government. Table 1 (attached) provides an overview of the policy application.

The Risk management guidelines provide guidance to agencies that are considering storing and processing Australian Government information in outsourced or offshore ICT arrangements – for example, using cloud computing services. The Risk management guidelines establish a whole-of-government approach to how different categories of information are treated when considering offshore or outsourced ICT arrangements.

The Risk management guidelines apply to most agencies as they apply to all agencies that implement the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM).

The Risk management guidelines form part of the PSPF and were developed by the Attorney-General's Department in consultation with the Australian Government Information Management Office, the Department of Broadband, Communications and the Digital Economy and the Australian Signals Directorate.

They are available through the PSPF website.

Why were Risk management guidelines developed?

Agencies have procured outsourced arrangements for storing and processing Australian Government information for several years and are actively examining cloud computing services for their possible efficiency, flexibility and lower costs.

The Risk management guidelines are intended to provide a consistent and structured approach to undertaking a risk assessment when considering outsourced or offshore ICT arrangements for Australian Government information. They are intended to assist government decision makers to evaluate the benefits of the adoption of cloud computing

services and assist agencies to consider the contextual risks specific to their agency and operating environment. The Risk management guidelines do not preclude the storage offshore of Australian Government information or prevent the adoption of cloud computing services by agencies.

What do the Risk management guidelines require?

Under the Risk management guidelines, agencies proposing that Australian Government information be held in outsourced or offshore arrangements are to document that they have calculated and accepted the associated security risks, where applicable, in accordance with the Risk management guidelines.

The Risk Management Guidelines provide information and advice to agencies in conducting this risk assessment process. Detailed guidance is provided on:

- the risk assessment framework
- establishing the strategic, organisational and security risk management contexts
- identifying, assessing and evaluating the risks
- finalising the risk assessment, including relevant approvals.

Agencies are not to enter into arrangements where the risk of outsourcing or storage offshore of Australian Government information cannot be quantified due to insufficient information or because the risks are too complex to be calculated.

More details for agencies on cloud computing policy and guidance are available on the AGIMO website.

The Australian Government Cloud Computing Policy provides whole-of-government direction to Australian Government agencies on their use of cloud computing services.

What should agencies do now?

Agencies considering adopting cloud computing or other outsourced or offshore arrangements for their government information will need to comply with the Risk management guidelines before entering into these arrangements. This will involve the agency conducting a risk assessment in accordance with the Risk management guidelines.

AGS can assist agencies in undertaking risk assessments in accordance with the Risk management guidelines. AGS is experienced in advising agencies on cloud computing and outsourcing issues and developed the *Negotiating the cloud – legal issues in cloud computing agreements* guide for AGIMO.

For further information please contact:

Tony Beal
Deputy General Counsel Commercial
T 02 6253 7231
tony.beal@ags.gov.au

Adrian Snooks
Senior Executive Lawyer
T 02 6253 7192
adrian.snooks@ags.gov.au

Kate Brophy
Senior Lawyer
T 02 9581 7678
kate.brophy@ags.gov.au

Swee-Kim Tan
Senior Lawyer
T 02 6253 7441
swee-kim.tan@ags.gov.au

Important: The material in *Express law* is provided to clients as an early, interim view for general information only, and further analysis on the matter may be prepared by AGS. The material should not be relied upon for the purpose of a particular matter. Please contact AGS before any action or decision is taken on the basis of any of the material in this message.

This message may contain confidential or legally privileged information. Only the addressee has the right to use or disseminate this information. If you think it was sent to you by mistake, please delete all copies and advise the sender. For the purposes of the *Spam Act 2003,* this email is authorised by AGS. Find out more about AGS at http://www.ags.gov.au.

If you do not wish to receive similar messages in the future, please reply to:
mailto:unsubscribe@ags.gov.au

Table 1: *Policy for the Storage and Processing of Australian Government information in Outsourced or Offshore Arrangements*

ICT Arrangement	Unclassified information that is publicly available	Other unclassified information that is not publicly available	All information requiring privacy protections[1]	Security classified information
Offshore and **Outsourced - Domestically hosted (onshore) public cloud**	Agencies can enter into these arrangements following a risk assessment. The handling, storage, transmission, transportation and disposal of information in these arrangements should be done in accordance with the *Australian Government Information security management protocol*.	Agencies can enter into these arrangements following a risk assessment. Agency heads must also document that they have calculated and accept the associated security risks as per the guidelines developed by the Attorney-General's Department.[2]	Agencies cannot enter into these arrangements, unless: 1) relevant portfolio Minister agrees that sufficient technological or other measures have been implemented to mitigate the risk of unauthorised access, and 2) there has been consultation with, and agreement from, the Minister	These guidelines do not focus on the controls for Australian Government security classified information which are detailed in the *Australian Government Information security management protocol* and Information Security Manual.

[1] Personal information as defined by the *Privacy Act 1988*

[2] Risk Management Guidelines for the Storage and Processing of Australian Government I(information in Outsources or Offshore ICT arrangements (these guidelines)

ICT Arrangement	Unclassified information that is publicly available	Other unclassified information that is not publicly available	All information requiring privacy protections[1]	Security classified information
			responsible for privacy and the security of Government information (the Attorney-General).	
Outsourced – Domestically hosted (onshore) private, internal or community cloud	Agencies can enter into these arrangements following a risk assessment. The handling, storage, transmission, transportation and disposal of information in these arrangements should be done in accordance with the *Australian Government Information security management protocol*.			