Australian Government

Information Management Office

Negotiating the cloud – legal issues in cloud computing agreements

Better Practice Guide

JULY 2012

AGIMO is part of the Department of Finance and Deregulation

Contents

Introduction

Like cloud computing itself, cloud computing agreements appear in a wide variety of forms. These can range from simple standardised click wrap agreements to multilayered sets of terms and conditions. There are, however, a core set of legal issues that agencies should consider in any cloud computing agreement, whether the agreement expressly deals with those issues or not.

The purpose of this Better Practice Guide is to assist agencies to navigate typical legal issues in cloud computing agreements. Some of these issues will be familiar to those who deal regularly with information technology contracts, but even in respect to those issues, the nature of cloud computing can create new or different risks and agencies may need to consider those issues afresh in the cloud computing context.

The Australian Government Information Management Office (AGIMO) is investigating potential Whole-of-Government procurement approaches for cloud computing during 2012. Agencies should monitor the AGIMO blog for further information.

Overview of cloud computing legal issues

What is cloud computing?

As set out in the *Cloud Computing Strategic Direction Paper*[1], the Australian Government defines cloud computing as:

> *an ICT sourcing and delivery model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

Cloud computing at the broadest level, therefore, is the provision of computing as a service over a network, typically the Internet.

Cloud computing services are usually grouped into the following categories:

- software as a service – the provision of software over a network rather than the software being loaded directly onto a locally available computer
- platform as a service – the provision of computing platforms that create the environment for other software to run (for example, operating systems) over a network rather than being loaded directly onto a locally available computer

[1] http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html

- infrastructure as a service – the provision of access to computer infrastructure (for example, data storage or processing capability) over a network that is used to compliment local platform resources.

Cloud computing is becoming an increasingly attractive model for delivery of an ever expanding range of hardware and software functionality, primarily due to the potential cost savings and enhanced flexibility that can be offered by cloud computing providers.

Cost savings can potentially be achieved as a result of the aggregation of hardware in large data centres and the ability of such centres to offer on-demand computing to cater for peaks and troughs in an agency's computing usage. Enhanced flexibility arises from the ability for users to access computing from a range of locations (courtesy of the Internet). This flexibility is bolstered by the increasing spread of wireless Internet connectivity and the proliferation of mobile Internet enabled devices that make mobile computing more attractive and accessible.

Deployment models

Cloud computing can be deployed in a number of ways including:

- public cloud (where access to the cloud computing service is not restricted to a particular entity or community of entities and is generally available to the public)
- private cloud (where access is restricted to a single private entity – for example a single agency)
- community cloud (where access is available for a community of entities – for example, a range of Australian Government agencies in a government community cloud)
- hybrid cloud (where more than one of the above models operate in tandem to provide some level of interactivity between the clouds that is not available outside of the hybrid cloud).

Obtaining cloud computing services

In the Commonwealth policy context, the process of obtaining cloud computing services would normally be classified as a procurement. As a result it will be necessary for an agency to meet all the usual requirements that apply to procurement, including compliance with:

- the Commonwealth Procurement Rules (CPRs)and, for FMA Act agencies:
- the agency's Chief Executive Instructions
- the Financial Management and Accountability (FMA) process.

In many cases, and particularly for large-scale cloud computing services, the Additional Rules of the CPRs are likely to be triggered. This means that cloud computing services will generally need to be obtained as the result of an open approach to the market and consequent evaluation process to select a preferred tenderer (or panel of providers).

How to use this guide

In some cases – for example where the services are offered only by one provider because of the need for particular proprietary software or hardware – agencies may have to deal with the legal agreements proposed by the provider. In other cases, agencies may be able to propose their own legal terms. In either situation, agencies should carefully consider the implications of the terms of the proposed agreement. This guide sets out some of these considerations.

In using the guide, agencies should be aware that:

- This guide canvasses typical issues in cloud computing legal agreements but other significant issues may exist in a specific agreement. Agencies should therefore always carefully review and obtain all necessary legal advice on the specific terms to use.
- Not all of the legal issues raised in this guide will be relevant to each cloud computing service. For example, some issues relating to the protection of information may be less important where the provider is not holding or accessing the agency's data.

The standard terms on which many cloud computing services are offered may not meet all of the legal requirements of an agency. As those requirements may impact on the price and delivery model for cloud computing services, it is important for an agency to raise the relevant issues and contractual positions (such as those set out in this guide) with providers early in the procurement process. This will assist the agency to negotiate an agreement that is acceptable to all parties.

The key legal issues addressed by this guide can be broken down into the following categories:

- protection of information
- liability
- performance management
- ending the arrangement
- dispute resolution
- other legal issues.

This guide also looks at the longer term issues associated with managing a cloud computing agreement over its life.

Key legal issues

Protection of information

Privacy

Information about the privacy obligations for Commonwealth contracts can be found on the Office of the Australian Information Commissioner's (OAIC) *website*[2]. Agencies are also strongly advised to consider the *Better Practice Guide – Privacy and Cloud Computing for Australian Government Agencies*[3] before entering into any cloud computing arrangement.

Cloud computing does not necessarily have to be privacy invasive, but moving data into the cloud means that the data will move outside of the direct control of the agency and may, in some instances, be processed and stored outside of Australia. Different levels of indirect control of this

[2] http://www.oaic.gov.au/

[3] http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html

data are possible depending on the type of cloud service selected and the legal protections put in place by the agency.

Agencies need to be aware of their privacy and data security obligations when transferring personal information into any cloud environment. If privacy issues cannot be adequately addressed, the OAIC advises that it will not be appropriate to transfer 'personal information' into a public cloud.

Section 95B of the *Privacy Act 1988* (Cth) requires agencies entering into contracts for the provision of services to the Commonwealth, to:

- take contractual measures to ensure contracted services providers do not do an act or engage in a practice that would breach any *Information Privacy Principles (IPPs)*[4]
- ensure agreements do not authorise providers or their subcontractors to do or engage in an act or practice that would breach any IPPs,

if done or engaged in by the agency itself.

In addition, agencies should ensure that the provider is contractually prohibited from using the data for any of the provider's own purposes – such as advertising or other commercial services – as this is likely to be inconsistent with the IPPs and the intentions of the agency in entering the agreement.

Agencies engaging cloud service providers need to take appropriate contractual measures to ensure personal information is protected, regardless of whether or not the provider (and any subcontractors) are based in Australia or overseas. When contracting offshore, agencies need to take particular care to ensure they are able to enforce the provisions of the agreement.

Agencies should also consider the practical implications of their Privacy Act obligations, including whether specific contractual measures enabling them to meet their obligations are required. For example, IPP 7 *Alteration of records containing personal information* requires agencies, where an individual's request to alter a record has been refused, to attach a statement to the record on request. Agencies would need to ensure that a cloud service provider is obliged to meet this requirement.

Security

Clearly one significant issue for any cloud computing agreement where the provider holds, or is able to access, an agency's data is the security of that data. This issue is heightened from a risk perspective where the data is sensitive (including personal information).

Agencies should refer to the Defence Signals Directorate's *Cloud Computing Security Considerations*[5] for detailed guidance on issues to consider from a security perspective. In following this guidance, agencies should develop a comprehensive risk assessment to make an informed decision on the suitability of adopting a cloud based solution and assess the appropriate security protections it requires. The following are contractual measures that may, depending on the circumstances including the type of cloud service used, be appropriate to include in an agreement for cloud computing services:

- where the service is to be provided from a location within Australia, a prohibition on the provider transmitting data outside of Australia without the prior approval of the agency

[4] http://www.privacy.gov.au/materials/types/infosheets/view/6541

[5] http://www.dsd.gov.au/infosec/cloudsecurity.htm

- the level of security and encryption to be applied to agency data held and transmitted by the provider
- the level of access security protocols to be implemented by the provider to defeat unauthorised attempts to access the data by third parties, provider personnel and other customers of the provider
- where physical media is damaged and replaced, requirements for the sanitisation or deletion of data in the damaged media
- the storage of separate packages of data – for example, it may be important to avoid the provider aggregating separate packages on the same hardware (as such aggregation may increase the sensitivity of data or risks to security of the information)
- a requirement for the provider to notify the agency immediately in the event of security incidents or intrusions, or requests from foreign government agencies for access to the data, to enable the agency to manage these events proactively
- a requirement for the provider to store data so as to prevent other customers of the provider from accessing the agency's data. For less sensitive data, logical separation supported by strong technical security measures (where data may be held on the same servers as other customer data) may be sufficient. If the data is more sensitive, storage on specified hardware that is unique to the agency may be appropriate so that there can be physical security precautions set up between the hardware storing the agency's information and other hardware held by the provider
- a requirement for the provider to destroy or sanitise (or de-identify in the case of personal information) sensitive information held by the provider at the end of the agreement, where such data is not or cannot be returned to the agency. This may need to extend to destruction of physical hardware on which such data is held to avoid risk that the data may be recovered
- specific security requirements depending on the nature of the service and the sensitivity of the data.

Confidentiality

An agency may have contractual, equitable or statutory obligations to keep particular information confidential. Therefore it is important that these obligations are also transmitted to the provider in circumstances where the provider is storing or accessing an agency's data.

In most cases, an agency will want a provider to meet a minimum level of confidentiality for the agency's information. In cases where the provider is obtaining access to particularly sensitive information, the level of protection will need to be significantly stronger. Agencies should consider in an agreement:

- the replication of any obligations placed upon the agency by contract or law
- for non-sensitive data, requirements to ensure the provider is aware of the level of confidentiality required and commits to protecting that data appropriately
- for sensitive data, more detailed confidentiality obligations. In some cases where an extra layer of protection is necessary, it may be appropriate to:
    - require the provider to obtain individual confidentiality deeds from their personnel
    - restrict access to the agency's data to a limited set of the provider's personnel only.

Where an agreement requires an agency to maintain provider information as confidential, agencies should be aware of Commonwealth policies which require:

- restricting the type of provider information that is subject to confidentiality

- the inclusion of standard Commonwealth exceptions to confidentiality including the right to provide information to the relevant minister as well as houses of Parliament.

Records management requirements

Agencies should refer to *Records management and the cloud - a checklist*[6] prepared by the National Archives of Australia for records management considerations in cloud computing. That advice requires agencies to include appropriate controls and protections (for example through agreement with the cloud service provider) that match the value of the records and address the risks of cloud computing for an agency's records.

Audit

All the protections described in this section may potentially be worthless unless the agency is able to confirm that required information protection requirements are in fact being met. Audit of cloud computing arrangements is one way of checking compliance. Audit of such arrangements is however potentially complicated by:

- the location of the data – which, unless specifically identified and locked down in the agreement, may be unknown to the agency, and could be located in one or more discrete sites in foreign countries
- the nature of cloud computing itself which may involve agency data being spread across a large number of different provider computing devices (in order to harness the economies of scale and on-demand provision of computing that cloud computing services offer).

As a result, agencies should consider including the following rights in any agreement:

- restricting the locations/countries in which agency data may be held (with movement to new locations permitted with advance approval in writing from the agency)
- rights to audit the provider's compliance with the agreement including rights of access to the provider's premises where relevant records and agency data is being held
- audit rights for the agency (or its nominee), the Auditor-General and the Information Commissioner
- a right for the agency to appoint a commercial auditor as its nominee (as this allows the agency to appoint an auditor in the same location as the provider's data centre to save costs and ensure compliance with relevant jurisdictional laws)
- where technically available, the right for the agency to remotely monitor access to its data and where this is not possible, a requirement that the provider maintain an audit log of access to the agency's data and provide that log to the agency on request.

Compensation for data loss/misuse

It is possible that data could be permanently lost by a cloud computing services provider in a number of circumstances such as technical or operator error as well as fire or other disasters. Similarly, there is always the risk of misuse of data by rogue employees of the provider or compromise by external parties.

While the probability of such problems can be minimised by the provider ensuring offsite data back-up, proper technical and security training and hardware maintenance, it is important for

[6] http://www.naa.gov.au/records-management/publications/cloud-checklist.aspx

an agency to consider how to address data loss or misuse in its agreement with the provider. This is particularly the case where the data is provided by third parties (such as members of the public) and the agency risks legal liability in the event data is unrecoverable or used inappropriately.

An agency, in determining the risks posed by a cloud computing arrangement, should consider which party is best placed to manage those risks and therefore whether the agreement with the cloud service provider should:

- require the provider to be responsible for indirect and consequential losses (which will typically be the type of losses that flow from data loss and misuse)
- include an indemnity from the provider in respect to data loss or misuse as a result of the negligent, illegal or wilfully wrong act or omission of the provider or its personnel
- have a separate liability cap for data loss or misuse that is sufficiently high to cover potential liability arising from such loss or misuse.

For more detail on the above terms, refer to the Liability section of this guide.

Subcontractors

A critical component of ensuring that an agency has proper protection for its information is to ensure, in the agreement with the provider, that any subcontractors of the provider are also obliged to meet the same requirements as the provider. If this is not done, an agency may find that any protections it has negotiated into the agreement with the provider do not end up giving it the desired protection where the services are carried out by subcontractors. It will also be important to know who a provider's subcontractors are so that an agency understands what companies may have access to the agency's systems and data.

Liability

Limitations on liability

In common with traditional information technology agreements, cloud service agreements typically seek to minimise the provider's liability for any loss that arises from the provision of the service. This may include:

- excluding indirect and consequential losses (such as data loss)
- setting low liability caps (typically equivalent to one year's fees under the agreement) or in some cases excluding liability entirely
- not excluding key types of liability from any liability cap.

Agencies should seek to comply with the Commonwealth's policy on capping supplier liability in information technology contracts (see *Finance Circular 2006/03*[7]) when negotiating limitations with providers. The starting point is that the Commonwealth will accept a cap on the provider's liability as a default position in information technology contracts provided that a list of exceptions to the cap is agreed by the provider. These exceptions are:

- personal injury (including sickness and death)
- loss or damage to tangible property
- breach of privacy, security or confidentiality obligations

[7] http://www.finance.gov.au/publications/finance-circulars/2006/03.html

- intellectual property infringement
- unlawful, or illegal, acts or omissions.

In addition to the standard exceptions, agencies should consider whether the risks of their procurement justify additional protection such as including the following as exceptions to a provider's liability cap:

- loss caused by service interruption
- data loss
- misuse of data.

Decisions made by agencies about the amount of any liability cap should be informed by a risk assessment that examines all identifiable potential liabilities and determines the likelihood and effect of such risks being realised.

Indemnity

An indemnity is a legally binding promise by which one party undertakes to accept the risk of loss or damage another party may suffer. In some cloud computing service agreements the provider will require an indemnity from the agency. These typically might include indemnities for:

- infringement of a third party's rights (including privacy and intellectual property rights) by the provider as a result of the provider's processing of third party data supplied by the agency
- any loss or damage arising from the agency's use of the service
- breach of the agreement by the agency.

Agreeing to give an indemnity may expose an agency to the risk of liability or costs that it would not otherwise be liable for. Indemnities given by an agency must comply with:

- the Commonwealth's indemnity guidelines – these guidelines make clear that agencies should only give indemnities where the expected benefits outweigh the level and cost of risk being accepted and that generally the party best placed to manage a risk should bear that risk
- the FMA Act and Regulations – an indemnity will form a contingent liability that may require an FMA agency to obtain agreement under FMA Regulation 10.

For further details on the handling of liability caps and indemnities, agencies can refer to Australian Government Solicitor (AGS) Legal Briefing [8].

Performance management

Service levels

Service levels are an important way of ensuring that a provider meets the level of service expected by the agency. This is particularly important where the cloud computing service is critical either to the functioning of an agency or to the agency's clients. There are three elements common to an effective service level regime:

[8] http://www.ags.gov.au/publications/legal-briefing/br93.pdf

- The service levels have to be meaningful – that is, they need to measure performance that is important to the agency.
- The provider's performance against service levels should be able to be easily measured and auditable.
- The incentive (whether stick or carrot or combination of both) for the provider to meet the service levels has to be sufficient to encourage performance at the required level. Any service level credits paid to an agency for the provider's failure to meet the service levels should not exceed a genuine pre-estimate of the loss to avoid being a penalty and therefore unenforceable.

It should come as no surprise that providers will generally only offer to meet service levels that they know are well within their performance capability and so considerable negotiation may be required for an agency to achieve levels that are suitable for its needs, where these exceed the standard commercial offerings.

Response times

Where an interruption to all or part of the service does occur, it will be important to contractually tie the provider to investigate and, where it is in the domain of the provider, resolve the interruption as soon as possible. An agency may wish to categorise response times based on the severity of the fault.

Flexibility of service

One of the key advantages of a cloud computing services model is that it should offer flexibility of service with the ability to easily scale up or down the required level of service depending on agency needs. It is therefore important for an agency to consider its requirements in this regard. Key issues to consider are:

- making sure that the pricing model is suitable – if the agency's demand for computing rises or falls, will the agency be required to pay higher prices (on a per unit basis) for the change in scale of the service?
- does the agreement allow for changes in the agency's demand to be easily implemented or will it require a potentially time consuming negotiation process?
- how will the agency ensure compliance with FMA Act requirements (for example, FMA Regulations 9 and 10) as a result of scalable service costs?

Business continuity and disaster recovery

Business continuity and disaster recovery will often be a critical consideration in cloud computing service agreements given the reliance that an agency may have on obtaining uninterrupted access to that service. Threats to business continuity in this context can include:

- interruption to communications networks
- hardware or software failure
- power failure
- disaster (fire, storm, riot etc) that disables access to the service.

Agencies should therefore consider including protections in their agreement with the provider where necessary to ensure access to the service is not disrupted. As an example, these could include:

- ensuring the provider has a geographically separate disaster recovery site with seamless transition
- ensuring the provider is able to operate in the event that mains power is disrupted (for example, use of Uninterruptible Power Supply and back-up generators)
- ensuring that business continuity is a strict requirement and not subject to qualifiers such as 'reasonable efforts'
- requiring a business continuity and disaster recovery plan be submitted for comment and approval by the agency
- limiting the right for the provider to suspend their service for force majeure reasons to circumstances where the business continuity and disaster recovery plan has been properly followed and implemented
- ensuring that scheduled maintenance outages of provider systems do not occur during hours that the agency requires access and use of the system (a common problem if the service is provided from a substantially different time zone).

Agencies may also need to take other precautions outside of the agreement (for example, in relation to their communications providers) to minimise disruptions (for example, issues with an agency's internet gateway) that are not the fault of the cloud computing provider. The provision of substantial services by way of the cloud could amplify the impact of any failures that occur in supporting contracts.

Ending the arrangement

Termination for convenience and early termination fees

As with all government contracts it is important to consider inclusion of an early termination clause (without the default of the provider) in the agreement that allows an agency to terminate or reduce the agreement at any time for any reason (these are often known as 'termination for convenience' clauses).

Where there is provision for early termination, agencies should consider what payments apply to the early termination. If compensation is appropriate, it should not exceed reasonable costs associated with the termination and would not, for example, extend to additional costs such as to cover loss of profit on the part of the provider. Significant early termination fees may act as a barrier to competition in the cloud services market and agencies may wish to consider this issue when determining whether to accept early termination fees or not.

Termination for default

An agency should ensure that it has the right to terminate for default where the provider does not meet the agency's reasonable requirements as set out in the agreement. The agency should also consider whether specific rights to terminate for default are required (for example, see the discussion of change of control in this guide).

Provider's right to terminate

Providers will ordinarily seek a right to terminate the agreement in certain circumstances, for example for agency default. In respect to any such right, the agency should consider including a sufficiently long notice period before the termination becomes effective to enable the agency to find a suitable alternative provider.

Legal advice on termination

Termination of any agreement is a serious matter and should only be undertaken, no matter how clear the wording of the agreement, following specific legal advice.

Disengagement/transition of services

Disengagement can be a key issue where the cloud computing services are critical services for the agency. In addition, easy and smooth disengagement and transition may ultimately lead in the longer term to greater competition and lower prices for cloud computing services to government as the barriers to transferring from one provider to another are reduced.

If an agency is transitioning to a new cloud computing services provider or alternatively bringing the services back in-house, then it will be important for the agency to consider including requirements in the agreement that the provider will:

- give all reasonable assistance in helping with the disengagement and transition including retrieval of all data in formats approved by the agency
- supply a detailed disengagement and transition plan to give the agency confidence in the nature and scope of the provider's disengagement services
- not delete any data at the end of the agreement without the express approval of the agency.

Dispute resolution

It is important to be clear about how disputes in relation to the cloud computing agreement will be resolved. Agencies should ensure that, at a minimum, the agreement states what country's (and jurisdiction's) laws apply to the agreement, which courts can hear disputes about the agreement (known as the choice of law provisions) and whether alternative dispute resolution mechanisms such as arbitration are proposed.

Even if carefully drafted choice of law provisions are included in an agreement, it will not necessarily preclude a court from applying different laws where the nominated laws, or forum, are not appropriate in the context of the relevant agreement or dispute.

'Choice of law' provisions may also have no effect on non-contractual legal issues that arise in the context of a cloud computing arrangement. For example, any contractual provision which purports to exclude the operation of a non-excludable warranty arising under the *Competition and Consumer Act 2010* (Cth) would be void under Australian law. The appropriate forum for hearing disputes about defamation or another civil wrong may also be determined without reference to any agreed contractual clause. Agencies should therefore consider seeking legal advice regarding all risks associated with cloud arrangements rather than just risks arising directly from the agreement.

Agencies should carefully consider the implications of choice of law provisions and proposed dispute resolution processes, particularly where such processes are compulsory. It may be necessary for agencies to obtain legal advice from lawyers in all relevant jurisdictions including the jurisdiction where the service is actually to be provided and the jurisdiction whose laws apply to the agreement. That advice may need to address potential costs, hidden risks and practical implications of the proposed arrangements.

Other legal issues

There are a range of other legal issues which may appear in a cloud computing services agreement.

Introduction of harmful code

A potential threat to an agency's systems and data will always be posed by harmful code (such as viruses and other malicious code). In the cloud computing environment, agencies will need to rely on the provider applying sufficient protection against the introduction of harmful code in hosted data and systems as well as via any communication with an agency's local systems. Agencies should therefore consider in each case the potential risks posed by harmful code and the relevant obligations that should be imposed on the provider to ensure that agency systems and data are protected.

Change of control and assignment/novation

It is critically important that an agency knows what entity it is entering into a cloud computing services agreement with and that it can control whether it allows another entity to obtain control of the initial provider. This is especially important where the provider stores sensitive data or provides services for sensitive computing tasks. There are, for example, some entities that the Australian Government is not permitted to contract with (for example, entities that Australia has agreed under international law not to deal with) and others that are deemed to pose a threat to the national security of Australia. Some ways of dealing with this issue include:

- requiring the provider to inform the agency in advance (subject to any listing rules of a relevant stock exchange) of any proposed change in control of the provider – such as changes in key management positions or changes in significant shareholders
- providing the agency with a right to terminate in the event that a change of control compromises the agency or the Australian Government
- requiring that any transfer of the provider's rights and obligations under the agreement to another entity (commonly referred to as 'assignment' in the case of rights and 'novation' in relation to rights and obligations) be subject to approval in advance by the agency
- requiring that any subcontractors be made known to the agency for consideration before the agreement is entered into and providing the agency with a right to approve the involvement of any new subcontractors.

Change of terms at discretion of the provider

Some cloud computing agreements, typically standardised services in the public cloud that are available to many customers, include clauses allowing the provider to change the terms of the agreement at any time at their sole discretion (that is, without input from the agency). From a commercial point of view, it is easy to understand why a provider may include such a clause – especially where it has many thousands of customers using the service. However, such a clause will create a very substantial risk for an agency, particularly if the agency has negotiated with the provider to include the types of clauses that are set out in this guide. As a result, agencies should consider either:

- deleting the right or making the right subject to the agency's agreement to any change, or
- ensuring that the provider is obliged to notify the agency well in advance of any changes and give the agency the right to terminate the agreement if it does not agree to the changes.

Application of foreign laws and transborder data transfer

Agencies should be aware that data stored by a cloud services provider may be subject to foreign laws (including where stored in Australia under the control of a provider subject to foreign

laws) as may data that is transferred internationally. Agencies should therefore carefully consider the impact of such laws when considering placing data into the cloud. For example:

- In certain circumstances, the US PATRIOT Act allows the US government to obtain data held anywhere in the world by US companies or companies with sufficient connections to the US. This would extend to data centres based in Australia that are operated by US companies and data centres based in the US operated by non-US companies.
- The European Community requires that transfers of personal data to third countries outside the EC must comply with the *EC Directive on Data Protection* which requires that third countries must be assessed as ensuring an adequate level of protection for the data.
- The European Commission has proposed new data protection laws that include a requirement that EU rules must apply if personal data is handled outside the EU by companies that are active in the EU market and offer their services to EU citizens. These proposed laws could therefore impact on how cloud providers treat their data holdings (including data held on behalf of Australian Government agencies). The proposed laws are yet to be considered by the European Parliament and agencies interested in the cloud should keep a watching brief on developments in this area.

Further issues

Agencies should closely check cloud service agreements to identify any other provisions that may be problematic. Examples of other potential legal issues that may need to be addressed include:

- *Freedom of Information Act 1982* (Cth) issues – the agency should ensure that the cloud services arrangement does not prevent it from complying with its obligations under the FOI Act. This would include ensuring that it can access the agency's data in the event that an FOI request is received and amend personal information in response to a request for amendment under the Privacy Act or FOI Act.
- Intellectual property ownership – the agency should ensure that the agreement does not transfer intellectual property ownership to the provider in any data stored by the provider on behalf of an agency.
- Publicity by the provider in respect of agreement – normally this would only be by agreement of an agency.
- Use of Commonwealth branding and logos by the provider – this is only permitted in accordance with the It's an Honour website[9] managed by the Department of the Prime Minister and Cabinet.
- Responsibility for end-users – agencies should be very careful about taking on responsibility for what public end users may do with data and applications made available to them through government websites and applications as the agency will generally have little or no control over the activities of end-users.
- Export controls – where data is provided across country borders (and back again) the agency will need to consider the impact of export control laws in the relevant jurisdictions which may impact on the type of data that may be provided to a cloud services provider and the country in which the cloud services provider operates. This is an evolving area that agencies should keep a watchful eye on.

[9] http://www.itsanhonour.gov.au/coat-arms/

- Requirement to take updates – agencies should ensure that any automatic updating of software that is required by the provider is consistent and compatible with existing agency systems.

Managing the agreement

The key issues to keep in mind in contract managing a cloud services agreement are:

- In the first place, make sure terms in the agreement are appropriate and reasonable for the agency, and if not, negotiate the amendment of those terms.
- Understand the terms of the agreement and keep a copy handy for reference during the life of the agreement.
- Be serious about enforcing the service level arrangements – monitor them closely and raise issues with the provider in the event of unsatisfactory service.
- Always be prepared to audit the provider, particularly if they are new to handling government clients. The reputation of government will be closely tied to how any providers may handle computing and data storage and transmission functions on behalf of government agencies.
- Within reasonable limits, maintain a good relationship with the provider so it is not necessary in all cases to have recourse to the agency's rights in the agreement.
- If things do go wrong, refer to the agreement so that the agency is aware of its contractual rights and obligations.
- Seek legal advice if an agency is unsure how to handle any issues that arise during the term of the agreement and in particular seek advice early if the agency is contemplating termination or other serious action in respect of the agreement.

Further information

Cloud computing policy guidance

- *Cloud Computing Strategic Direction Paper*
- *AGIMO Circular No 2011/001: Cloud Computing Policy and Cloud Computing Strategic Direction*
- *Cloud Computing Security Considerations*
- *Better Practice Guide – Privacy and Cloud Computing for Australian Government Agencies*
- *Records Management and the cloud - a checklist*.

General legal guidance

- AGS Legal Briefing *Indemnities in Commonwealth Contracting* (19 August 2011).

Legal checklist

The following checklist identifies the legal issues discussed in the guide. In contemplating a cloud computing procurement, an agency should ensure that these issues are considered and addressed as necessary. Please note that a particular cloud computing procurement or agreement may raise additional legal issues as well. Agencies should always ensure that they have properly reviewed, and obtained all necessary specific legal advice on, any agreement they wish to enter.

Protection of information

- ☐ privacy
- ☐ security
- ☐ confidentiality
- ☐ records management requirements
- ☐ audit
- ☐ compensation for data loss/misuse
- ☐ subcontractors

Liability

- ☐ limitations on liability
- ☐ indemnity

Performance management

- ☐ service levels
- ☐ response times
- ☐ flexibility of service
- ☐ business continuity and disaster recovery

Ending the arrangement

- ☐ termination for convenience and early termination fees
- ☐ termination for default
- ☐ provider's right to terminate
- ☐ legal advice on termination
- ☐ disengagement/transition of services

Dispute resolution

- ☐ choice of law

Other legal issues

- ☐ introduction of harmful code
- ☐ change of control and assignment/novation
- ☐ change of terms at discretion of the provider
- ☐ application of foreign laws and transborder data transfer
- ☐ further issues:
  - ☐ Freedom of Information Act 1982 obligations
  - ☐ intellectual property ownership
  - ☐ publicity by the provider in respect of agreement
  - ☐ use of Commonwealth branding and logos by the provider
  - ☐ responsibility for end-users
  - ☐ export controls
  - ☐ requirement to take updates

Managing the agreement

- ☐ ensure that agreement terms are appropriate and reasonable
- ☐ understand the terms of the agreement and keep a copy handy
- ☐ enforce the service level arrangements
- ☐ be prepared to audit the provider
- ☐ within reasonable limits, maintain a good relationship with the provider
- ☐ if things go wrong, be aware of contractual rights and obligations
- ☐ seek legal advice if difficult issues arise

Acknowledgments

This guide was written and developed for AGIMO by Adrian Snooks, Senior Executive Lawyer at the Australian Government Solicitor (AGS) with contributions on privacy and dispute resolution from Andrew Schatz, Senior Lawyer.

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

Disclaimer

This guide discusses typical legal issues found in a sample of cloud computing agreements available at the time of its publication and is not intended to be comprehensive in its treatment of those issues or possible solutions. This guide must not be relied upon as legal advice for any specific situation. Agencies should always ensure that they have properly reviewed, and obtained all necessary specific legal advice on, any agreement they wish to enter.

Copyright notice

ISBN 978-1-922096-05-0 online