THE LAW SOCIETY
OF SOUTH AUSTRALIA
THE VOICE OF THE SOUTH AUSTRALIAN LEGAL PROFESSION

Cloud Computing Guidelines for Legal Practitioners

The purpose of these Guidelines is to provide practitioners with a starting point for seeking general information about their professional obligations. They are not an exhaustive statement of all the relevant professional obligations that might apply to specific circumstances.

These Guidelines are not intended to, and do not, replace or amend a legal practitioner's obligations under the Australian Solicitors' Conduct Rules.

If you need advice that addresses a specific set of facts, please contact Ethics and Practice on 8229 0229.

Introduction

1. Law practices are increasingly using cloud storage and software systems as an alternative to in-house data storage and IT programmes.
2. The cloud has a number of advantages – particularly flexibility and cost – but these have to be balanced with risks to privacy and control.
3. Legal practitioners are required to protect and hold in strict confidence all information concerning a client acquired in the course of the professional relationship.
4. These Guidelines aim to give legal practitioners some helpful guidance on best practices for using the cloud. They do not constitute an endorsement of a particular product or service.

What is cloud computing?

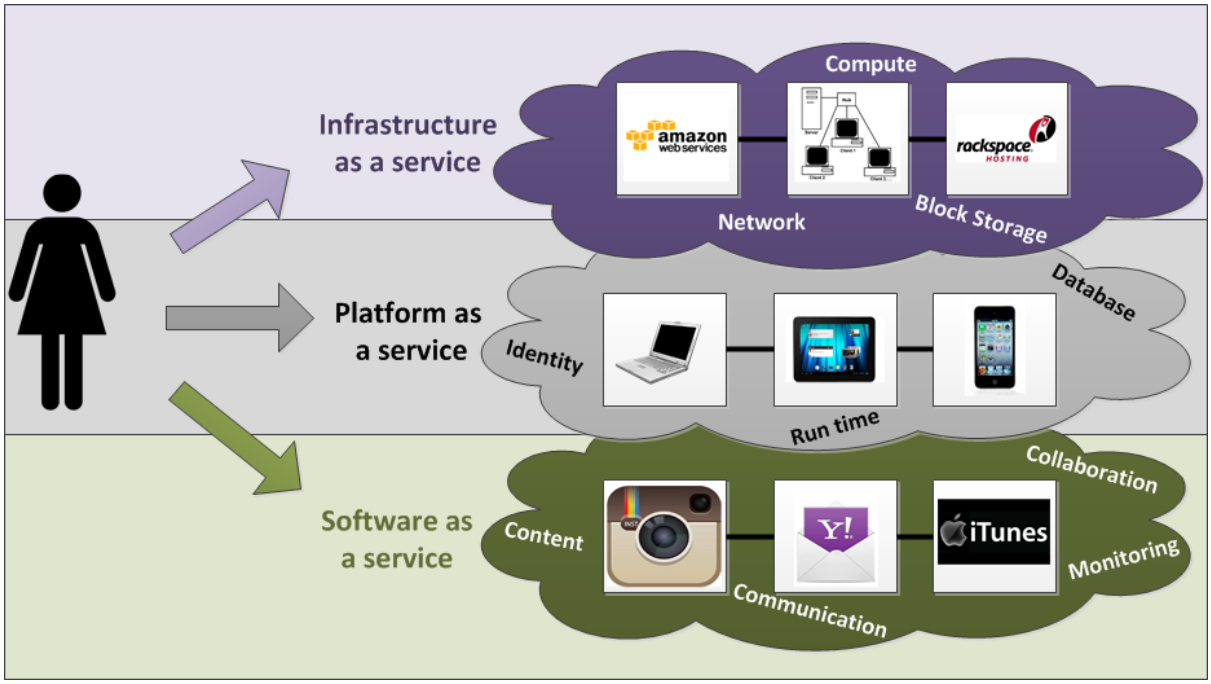
5. There is no universally accepted definition of cloud computing. In simple terms there are many clouds, each of which is an IT service accessed through the Internet. Each cloud is a network of servers that are accessed via the Internet instead of a law practice's office network server or the hard drive on an individual computer.
6. The Australian government has adopted the following definition of cloud computing published by the National Institute of Standards and Technology (NIST), which is part of the U.S Department of Commerce:

   Cloud computing is a 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. . [i]

7. From a consumer's perspective the essential characteristic of cloud computing is that computing resources are accessed automatically over a network, which will be the Internet for most people. The computing resources being used and the device from which they are being accessed are separate. For example, while your tablet will have an operating system it might not have any word processing software installed on it. However, you could still do word processing by using a word processing service offered by a provider over the Internet.
8. The word processing software would be located on the service provider's ICT infrastructure. Once you have finished your document you could store it on storage accessed over the Internet. Unless you made a backup copy on your tablet, your document would be stored on the relevant service provider's ICT infrastructure only. When you wanted to access the document again you would retrieve it over the Internet.
9. The essential characteristics from a service provider's perspective are:
    - pooled ICT infrastructure and applications that can service multiple consumers;
    - computing resources provided can rapidly match changes in demand for them; and
    - an ability to measure the computing resources being used and to use measurements to control and optimise their provision.
10. The use of the word 'cloud' suggests that computing resources accessed over it do not have a physical location. This is not true. Typically, computing resources are located at datacentres. Datacentres contain the underlying ICT infrastructure and applications necessary to provide computing resources to consumers. This includes server computers, operating systems, network systems, storage and software applications. Importantly, datacentres can be located anywhere in the world.
11. This is an essential consideration for legal practitioners because foreign laws will apply to data stored on datacentres located in foreign jurisdictions. In these Guidelines the term 'cloud infrastructure' is used to refer to the ICT infrastructure that meets these essential characteristics.
12. The service models are: Software as a Service (***SaaS***); Platform as a Service (***PaaS***); and Infrastructure as a Service (***IaaS***). Most relevant for legal practitioners and law practices will be SaaS and IaaS.

Figure 1 Cloud service categories

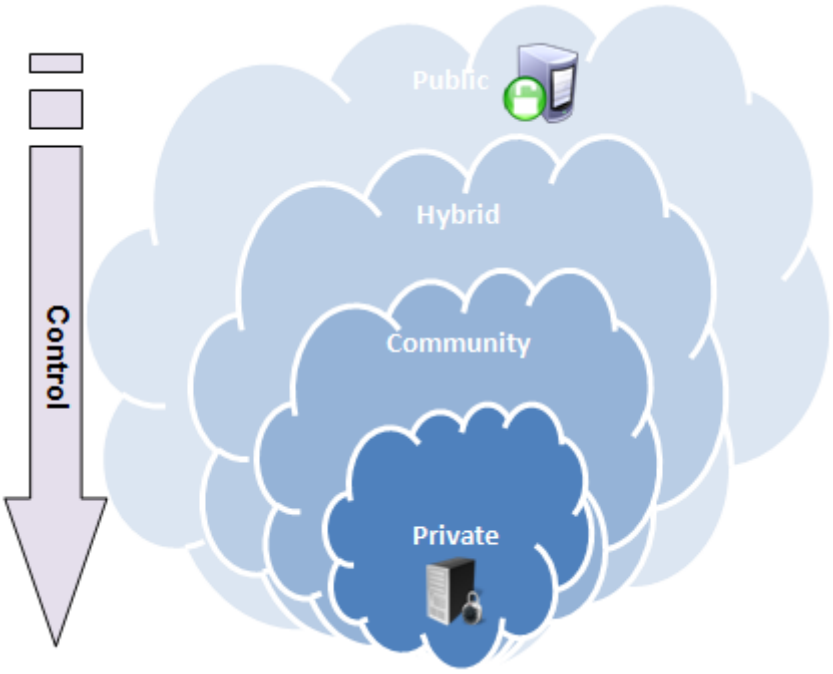


Source: ACMA, The cloud—services, computing and digital data: Emerging issues in media and communications, Occasional paper 3.

- ***SaaS*** is where the consumer accesses a service provider's applications that are running on cloud infrastructure. Common consumer oriented examples include: web browser email services; cloud storage services; many smartphone apps; and social networking services. A common business oriented example is customer relationship management software. Example SaaS vendor services include Salesforce.com Customer Relationship Management (CRM), Google Docs and Google Gmail. Microsoft Office 365 (formerly called Business Productivity Online Suite) consists of Microsoft Office Web Apps, Microsoft Exchange Online, Microsoft SharePoint Online, Microsoft Dynamics CRM Online and Microsoft Lync.
- ***IaaS*** is where a consumer can access a service provider's cloud infrastructure as an on-demand service. Instead of owning and operating server computers, storage, network systems and operating systems a consumer can access, use and pay for these things as a service. Example IaaS vendor services include Amazon Elastic Compute Cloud (EC2), GoGrid and Rackspace Cloud.
- ***PaaS*** is where the consumer can create or acquire applications created using resources supported by the service provider and then use, or offer for use, those applications. It is mostly relevant for software development. Example PaaS vendor services include Google App Engine, Force.com, Amazon Web Services Elastic Beanstalk and the Microsoft Windows Azure platform.

13. The four deployment models are: private cloud; public cloud; hybrid cloud; community cloud.

Figure 2 Main models of cloud computing in use in Australia



Source: ACMA, The cloud—services, computing and digital data: Emerging issues in media and communications, Occasional paper 3.

14. Each model describes a level of access to cloud infrastructure. In a **private** cloud the cloud infrastructure is provisioned for a single entity. In contrast, in the **public** cloud the cloud infrastructure is provisioned for the general public. This guidance is concerned with the public cloud only. The Society considers it likely that most legal practitioners and law practices considering cloud computing services will be considering services on the public cloud. In practice this means paying a third party service provider to use particular cloud computing services that are accessed over the Internet.

15. A vendor adding the words 'cloud' or 'as a Service' to the names of their products and services does not automatically mean that the vendor is selling cloud computing as per the NIST definition above.

16. In Australia, there are many cloud computing service providers providing on-demand information and communications technology services such as Ninefold and Ultraserve. Overseas cloud service providers are increasingly locating data centres in Australia (for example, IBM, Rackspace, Dell, Hewlett Packard and Amazon), or partnering with local businesses to provide locally based servers (Microsoft for example).

17. It is also important to understand that cloud storage and sync is not the same as online backup. If your cloud storage solution has been configured to enable 'two-way sync' (that is, changes such as deleting a file on either your local office computer or deleting a file on

the cloud storage) could mean that data could be lost from both storage locations. Also, most cloud services do not offer fine revision histories for the files you sync, a feature that is critical to a good backup service. It is important to keep more than one backup of your data, including one that is offsite. Using an online backup service means that your data is kept regularly updated, complete with granular revisions, stored and encrypted in someone else's datacentre, where it is also regularly updated. It is also recommended to store backups on an external hard drive or a network attached storage (NAS), especially for quick restores if your system suffers an outage and requires immediate restoration of data. When it comes to online backup, find a suitable device that is easy to set up and offers strong encryption.

18. The type of encryption utilised varies from provider to provider. More information regarding the type of encryption used can often be found in an information security policy of the cloud providers website.

19. An information security policy will also typically outline the type of security compliance that the provider has undertaken to ensure that data is protected and preserved with integrity. Note that the omission of such statements on a cloud providers website may not necessarily mean that they do not offer encryption or adhere to best security compliance practices. They may also be contained within a Service Level Agreement (SLA) or contract. Independent enquiries should be made with the cloud provider to determine if they are suitable for your needs.

Professional Obligations

20. Legal practitioners need to be aware of their professional obligations when it comes to the storage of, and access to, data in the cloud.

21. The Society's Guidelines on the retention and storage of testamentary and non-testamentary client files should be consulted at for a detailed analysis of the full range of professional obligations that arise with respect to client confidential information.

22. The professional obligations which are of particular note when it comes to cloud storage are as follows:

    a. Delivery of legal services competently and diligently (ASCR 4.1.3).

    b. Maintenance of confidentiality (ASCR 9).

    c. Return of client documents (ASCR 14).

23. Any move to using cloud services cannot compromise these obligations. All use of cloud computing by legal practitioners and law practices must enable compliance with the relevant conduct rules and also the *Privacy Act 1988* (Cth) (Privacy Act). Practitioners must ensure that the arrangements they enter into for the use of cloud storage enable them to comply with these requirements.

24. A breach of any professional obligation that arises from a practitioner's failure to ensure compliance, even if that failure is due to an innocent mistake, lack of understanding or technical error, could have the following ramifications:

    a. Disciplinary action for unsatisfactory professional conduct or professional misconduct.

    b. Claims of damages for negligence.

ASCR 4.1.3 - Requirement to deliver legal services competently and diligently

25. Legal practitioners have a fundamental ethical obligation to deliver legal services competently, diligently, and in a timely manner.

26. To maximise compliance with this requirement practitioners using the cloud should do the following:

    a. Maintain effective control of data stored on cloud computing services.

    b. Ensure adequate reliability of applications and access to data.

    c. Ensure adequate security of data.

    d. Ensure they are aware of where the data is geographically held and the foreign jurisdictional implications as such.

27. It is not possible to guarantee control of data, reliability of access to applications and data, and security of data when using cloud computing services (it is also not possible to guarantee such things in a local area network with a connection to the Internet). Risks of loss of control of data, loss of access to data or applications, and security breaches will always be present. Australian government policy for agencies considering the suitability of cloud computing services is to carry out a risk assessment. This assessment is set out in detail *in 'Cloud Computing Security for Cloud Service Providers'*[ii]. Legal practitioners should consult this document to carry out their own risk assessment.

28. Legal practitioners should be satisfied that they can maintain effective control of data. Relevant considerations include:

    a. Who owns the data once it is stored on a cloud service?

    b. Can you remove data from the service? That includes being able to delete data and any backup copies of the data.

    c. Can you transfer data from one service provider to another, or back to your own ICT infrastructure?

    d. Are there any cost implications as a result of obtaining or transferring data from a cloud provider? Can the cost implications be managed from the practices point of view?

29. There are technical and legal aspects to these considerations. On the one hand for example, the format data is stored in may have an impact on a legal practitioner's ability to transfer it. And on the other, the agreement between the legal practitioner and service provider may or may not address these considerations.

30. Legal practitioners should be satisfied that any cloud computing service will be adequately reliable (which should also include their own access to a cloud computing service). It may be difficult to deliver legal services at all if you cannot access client documents and your email. It will probably be difficult to make an independent technical assessment of reliability. Other ways to try and ensure reliability include considering services from reputable providers only, and to review proposed service agreements to see whether they contain any relevant terms. Many cloud service providers provide service level guarantees for 'up-time'. That is, time that the relevant service is available. These guarantees vary so legal practitioners should take the time to understand what exactly is being guaranteed, and also whether the guarantee forms part of the service agreement.

31. Legal practitioners should also consider ways that they can continue to deliver legal services should the cloud service become unavailable. In the case of cloud storage, one such measure is to backup copies of documents stored on a cloud service to an accessible device off the cloud. Legal practitioners should be aware of alternative access to internet services in the event their data service is interrupted by way of a business continuity plan that deals with internet outages. Devices such as mobile hotspot devices could be utilised in the event internet access to your office is interrupted.

32. Legal practitioners should also be satisfied that any cloud computing service will be sufficiently secure. It is here that the risks of using cloud computing services are particularly relevant. Again, it will probably be difficult to make an independent technical assessment of security of a service provider's cloud infrastructure but there are still things to look for, including:

    a. Whether the service provider encrypts data while in transmission and while at rest - i.e., when stored on its server computers.

    b. The robustness of authentication requirements to log-on to services (i.e. is there the ability to enable multi-factor authentication (MFA) to access the service?)

    c. Whether backups are carried out and how often they are carried out. Are the backups also retained within the same geographical jurisdiction as the service?

    d. Whether the service provider tests and audits its systems.

    e. Whether the service provider has any recognised accreditations or certifications.

    f. Security arrangements for the service provider's physical premises.

g. Cyber security arrangements, including as between the service provider's virtual server computers (where one physical server computer can operate in effect as several server computers).

h. Redundancy arrangements – i.e., arrangements to ensure that a service can continue to operate if utilities fail or if part of the service provider's ICT infrastructure fails.

ASCR 9 - Requirement not to disclose confidential information

33. Rule 9 outlines a legal practitioner's fundamental obligations to not disclose information confidential to a client unless authorised or otherwise permitted to do so. A legal practitioner has a duty to protect and to hold in strict confidence all information concerning a client, the retainer, and the client's business and affairs acquired in the course of the professional relationship. The obligation of confidentiality continues indefinitely after the person has ceased to be the practitioner's client.

34. Using a cloud computing service to store documents containing client information may result in a disclosure of that information to the service provider.

35. There are two aspects to this issue; a technical one and a legal one.

36. The *technical* aspect is that once a document is stored on cloud storage service, the service provider will be able to access it. The only exception to this is if the consumer encrypts the document before storing it (this is different to the service provider encrypting the document). Assuming the service provider can access a document stored on its service, the *legal* aspect is whether the service provider agrees not to access documents stored on the service and to take steps to maintain confidentiality. The proposed agreement between a consumer and a service provider may provide that the service provider can access and use documents stored on the service for certain purposes.

37. Many standard agreements for consumer-oriented cloud storage providers provide that the service provider has the right to access documents for the purpose of providing the service and also if it is compelled to provide access to authorities. Service providers may also be exposed to confidential information in the event support is required with the service. Often service providers will provide on demand support that requires remote desktop access to your machine. A consequence of this remote desktop access is that often support involves showing help desk operators where a problem exists which typically may include inadvertently showing confidential information in the process.

38. Assuming the service provider can access a document stored on its service, the proposed agreement becomes an important consideration. If under that agreement the service provider can access documents you store on its service and there is no confidentiality obligation then information confidential to your client may be disclosed to the service provider. In addition, the service provider may not be under an obligation to advise you when it proposes to access your documents. While audit logs (dependent on the

application) could be used to determine user access to a file (that is, users of a practice that have access to the service), there is no guarantee that system administrators of the service will be shown in the audit log history.

39. In these circumstances, unless a legal practitioner takes other steps to ensure that a cloud storage service provider cannot access documents stored on its service, they should advise clients in writing proposing to store documents containing client information with a cloud storage provider, and that it is possible that client information will be disclosed to the provider.

40. Inadvertent disclosure of client information by a data breach or a breach of security that occurs on the service provider's cloud infrastructure is a separate issue. Legal practitioners should advise their clients in writing that there is a risk that client information stored on a cloud storage provider may be disclosed in this way.

ASCR 14 - Requirement to return client documents

41. Rule 14 outlines the requirement for law practices to return client documents at the end of an engagement, upon request and where there is no lien over the documents. The requirement to return client documents in the context of cloud computing services means being able to permanently remove copies of client documents stored on a service. A legal practitioner may not be able to do this if they do not have effective control of data stored on cloud computing services. The same considerations apply.

42. It is also important for law practices to be mindful of its requirements for retaining any record or information after the finalisation of the matter/engagement to which the record relates for 7 years, as per Rule 14 and Regulation 48 of the *Legal Practitioners Regulations 2014* (except where there are client instructions or legislation to the contrary). See paragraph 19 above and the Society's Guidelines on the retention and storage of testamentary and non-testamentary client files.

Meeting your IT needs

43. When initially considering using the cloud for data storage it is important to assess your law practice's IT needs, priorities and long term plan. For instance:

    a. What do you want your systems to do for you?

    b. Do your storage needs fluctuate?

    c. Do you need to be able to access your server/servers from multiple locations and multiple devices?

    d. What do your clients expect when they trust you with their personal information?

    e. Has your own IT infrastructure been audited by an IT professional to ensure that it is secure against digital threats?

44. The table below contains a list of benefits and risks associated with cloud computing. This list is indicative and not comprehensive.

Benefits	Risks
improved backup/disaster recovery	Security (provider and practitioner)
flexibility and agility	privacy breaches
increased storage capacity	cross-border privacy legislation
increased data handling capacity	service reliability and stability
reduced infrastructure costs	lack of control over customisation and integration
avoiding frequent updates to software	customer service
reduced internal IT staff costs	speed and bandwidth
economies of scale	danger of supplier lock-in
potentially more secure due to more expert staffing	difficulty achieving executive buy-in
better quality servers	client's insecurities about privacy risks

Cloud computing contract considerations

45. Cloud computing contracts vary widely. A good starting point is the Australian Government's Information Management Office's Better Practice Guide – *Negotiating the cloud – legal issues in cloud computing* agreements.[iii]

Cloud computing contract negotiation

46. It used to be that service providers called all the shots. However, in an increasingly competitive market some cloud computing providers are willing to adapt their terms and conditions for big clients. Small Australian cloud service providers may be willing to tailor a service to fit your needs, but these providers may not offer the financial and technology security of the bigger but less transparent or negotiable service providers.

Service provider reliability

47. The IT industry attracts some questionable providers. When choosing a cloud provider it is extremely important that you look closely at the providers for:

- track record and reputation;

- commitment to the cloud computing market;
- existing customers;
- financial position, provisions in place if the company goes bankrupt; and
- what will happen to your law practice's data if things go wrong.

48. In any contractual agreement it is important to be thorough. Cloud computing contracts involve a unique range of issues to be considered including the following:

    a. ***Service level agreements***: Contracts concerning cloud service availability are most commonly governed by SLAs which often provide a guarantee of the percentage of time for which the service will be operational. Service levels are an important way of ensuring that a provider meets the level of service expected by the law practice. This is particularly important where the cloud computing service is critical either to the functioning of a law practice or to its clients.

    There are three elements common to an effective service level regime:

    - the service levels have to be meaningful – i.e., they need to measure performance that is important to the law practice;
    - 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 a law practice 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.

    Providers will generally only offer to meet service levels that they know are well within their performance capability, and as such considerable negotiation may be required for a law practice to achieve levels that are suitable for its needs, where these exceed the standard commercial offerings.

    The remedy for failure to meet the guarantee is typically a service credit provided to the customer to offset fees for the month in question.

    However, some down time is often not included in that calculation. This includes scheduled maintenance; force majeure events; outage resulting from misuse of the service; and outages elsewhere on the Internet. Some include an exorbitant list of down-time excuses.

    SLAs must be scrutinised carefully to determine their overall effect and so that law practices are aware of the requirements to be met in order to seek service credits. And that these are reasonable.

For more information, refer to the Microsoft Cloud Services Due Diligence Checklist.[iv]

b. ***Service changes***: You should ensure that:

- the company is contractually obligated to inform you of any structural changes to the business in advance;
- you are able to terminate your contract under ownership changes;
- your data cannot be held in receivership;
- contracts cannot be changed without informing you and giving you the right to terminate the contract; and
- the provider cannot suspend service without prior notice, agreement, and good faith – unless in specific circumstances, such as for non-payment.

c. ***Subcontractors***: Ensure that you are aware where your data will journey at all times, and that your provider and (if relevant) subcontractors cannot access your client's data. You should also be clear on the rules surrounding subcontracting – whether it is permissible and what your involvement should be in the process. This may extend to services offered such as troubleshooting services (remote desktop help desk support), payment providers (in application invoice generation and payment platform) and other contractors/services relied on for the provision of the service.

d. ***Commercial gain***: Some cloud providers sell data to third parties. You need to take precautions that your provider will not access or sell your data.

e. ***Location of data***: Legal practitioners should be aware of where their data is located and the privacy laws in the jurisdiction where their data is being stored. The answer is in the terms and conditions and privacy policy of the cloud's host. If in doubt, it is recommended that legal practitioners ask their cloud host. Some hosts use servers all around the world, while others specialise in providing local clouds based entirely in Australia. Similarly, some providers may primarily host their services in Australia however their backups are retained in another part of the world due to the reduced cost in storing large amounts of data.

Australian-based clouds have traditionally been more expensive than international clouds, but this may change with increasing competition in the cloud market.

If the cloud service provider is unwilling to tell you the exact location of their data storage facilities, they need to be able to provide evidence of binding contractual commitments they have made to keep data in locations which won't compromise the privacy of their customers.

It is recommended that the following location information is sought from a cloud computing provider:

- whether there is a privacy law that applies in the country or countries where your data is stored or processed;
- whether that privacy law is similar to Australia's privacy law;
- whether the law applies to the cloud provider and to your information (some privacy laws exempt some types of businesses, or do not apply to the personal information of foreigners);
- how the cloud provider will deal with any requests for information that it receives from government agencies, courts etc. For example will the provider only disclose information in response to a court order? Will the provider let you know if it has to disclose information in response to a request?;
- will the cloud provider notify you if data is lost or stolen, for instance if the provider is hacked?; Similarly, is the provider required to adhere to the Notifiable Data Breach laws pursuant to the *Privacy Act*?[v]
- who can you or your clients complain to if there is a breach of privacy?

f. ***Lawful third party access to data***: International and domestic police or intelligence agencies can in certain circumstances lawfully obtain access to your data via your cloud service provider. However, it is important to remember that there are also times when international and domestic police or intelligence agencies can legally access data stored on your own server.

   It is important to research the systems that a cloud service provider uses to deal with requests for information from government agencies and how they validate the legality of the requests. You should have a clear understanding with appropriate contractual and operational process in place to cover how the cloud service provider will deal with a request to access your data.

   If a legal practitioner has concerns in respect of a certain client or class of client in respect of potential jurisdictional, privilege and third party access issues, that may be a matter requiring serious consideration before choosing to store client information in the cloud.

g. ***Getting data out***: You need to be able to get your information out and ensure it is no longer retained on the provider's servers once you are gone.

   The provider should state:

   - whether you can take the information with you if you choose not to use the service any longer;
   - whether the information will be returned in a format that you can use elsewhere – and the timeframes it will be returned in;

- who will bear the cost for the process of switching to a new supplier (generally the practitioner/practice would be liable for costs incurred in transferring or retrieving large quantities of data from a service provider);
- whether information will be kept on the provider's systems after you move on, or whether it will be securely deleted. For instance, many providers will hold backups which will keep records for a certain period even once an account is deleted; and
- how the provider will verify for you that the information has been deleted.

h. ***Use of integrated payment platforms:*** Legal practice management software has evolved to now include methods for invoices to be made directly to third parties.

Upon receipt of an invoice, payment can also be made utilising an integrated third-party payment platform (such as Stripe, RapidPay and others) to provide an easy method of billing without relying on traditional business banking practices. In practice, a practitioner would issue an invoice which is sent by email through to a third-party requesting payment be made which includes the ability to pay by electronic funds transfer or credit card payments.

In 2023, the South Australian Professional Indemnity Insurance Scheme was updated to impose a double excess payable of the amount set in the Certificate of Insurance if a claim arises out of any payment or electronic funds transfer for which the insured did not take reasonable steps to verify payment information.

It would be prudent for practices that rely on this payment method to ensure that payment information is verified prior to a payment being made, as interception and malicious amendment of emails is a common tactic used by criminals to defraud businesses and individuals.

i. ***Viruses, hackers and other criminal matters***: A legal practitioner must take all reasonable steps to prevent any person perpetrating a crime or fraud through their law practice. This includes taking reasonable steps to ensure the security of and access to electronic systems and passwords. It is recommended that an IT infrastructure security audit is undertaken regularly, and security controls are implemented to reduce the risk of unauthorised access.

j. ***Overall Customer Service:*** Some service agreements may state the minimum expected time to resolve an issue in the event a user is unable or is having difficulty in accessing the service or a feature of the service. Some helpdesks only provide assistance during specific times (i.e. business hours) or within a certain time frame (e.g. within 24 hours) which may impact on a practitioner's duty to competently and diligently provide for the delivery of legal services (ASCR 4.1.3).

General checklist

49. The following checklist may assist legal practitioners to address many of the issues referred to in this document.

- Reminder: cloud storage and sync is not the same as online backup. It is important to keep more than one backup of your data, including one that is offsite, which is:
    - air-gapped, that is disconnected from the computer when a back up is not being made or used;
    - encrypted;
    - periodically made; and
    - tested regularly to ensure the integrity of the data.
- Different cloud services carry different risks and responsibilities. How secure is your current system with handling personal information. Would it be safer stored with a trustworthy cloud provider?
- Encrypt data so it is protected both while it travels and when it's at the provider's end. Make sure your client's data will not be seen by any third parties.
- Research your provider thoroughly, online and via contacts. Read and compare providers' terms and conditions. Check what the expected time frame is for assistance from a service providers help desk may be in the event of a technical issue.
- See what legal jurisdiction's privacy laws a cloud provider operates under and what/if any non-government standards they have committed to.
- Know where your data is going to be stored and what privacy laws apply.
- Ask how you will be informed if your data has been compromised and what the protocols around this are.
- A cloud provider should use third party auditors to ensure compliance.
- Ability to exit: can you delete information and easily take it with you to another provider if you choose to. Be mindful of costs associated with this.
- Check what will happen to your data if the business goes bankrupt.
- Remember that you are responsible if your client's privacy is breached.

Useful resources

50. The Australian government has published a number of useful cloud computing resources online.

51. These guidelines have already referred to:*' Cloud Computing Security for Cloud Service Providers'*. Others include *'Cloud Computing Security for Tenants'*..[vi]

52. As detailed by the Office of the Australian Information Commissioner (OIAC),[vii] if an organisation is covered by the Privacy Act it must ensure that all the personal information it handles complies with the Australian Privacy Principles,[viii] including information in the cloud. Different considerations may apply depending on whether the client's information is stored in an Australian cloud or at an international location.

53. Given the diversity of cloud services, and the many ways in which they are used, it is not possible for the OAIC to give prescriptive rules about when use of a cloud service may or may not breach a client's privacy. Before signing up for cloud services, or providing a client's personal information, legal practitioners are recommended to read the cloud provider's privacy policy.

54. The Department of Communications has a fact sheet[ix] which discusses some of the privacy and security issues relating to cloud computing and lists some key questions legal practitioners should ask their cloud service provider.

55. The Australian Cyber Security Centre has a list of publications on securing the use of cloud computing services.[x]

Purpose of these guidelines

It is important to stress that these Guidelines are not rules of conduct and do not have the force of law. They are for the purpose of highlighting issues and considerations relating to practitioners adopting cloud computing for their law practice.

A failure to comply with the recommendations in these Guidelines does not of itself constitute misconduct on the part of a legal practitioner. It is where a practitioner has demonstrably breached his or her obligations that the issue of misconduct arises. The Guidelines merely assist in identifying risky practices and providing solutions for practitioners.

If you have any questions about these Guidelines please call Ethics and Practice on 8229 0229.

Last reviewed: August 2023

---

[i] https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

[ii] https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance/cloud-computing-security-cloud-service-providersaccessed on 20 January 2016

[iii] http://ict-industry-reports.com.au/wp-content/uploads/sites/4/2013/05/2013-Negotiating-The-Cloud-Legal-Assues-v1.1-AGIMO-Feb-2013.pdf (Feb 2013) accessed on 20 January 2016

[iv] https://www.microsoft.com/en-au/trust-center/compliance/due-diligence-checklist

[v] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)

[vi] https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance/cloud-computing-security-tenants

[vii] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information accessed on 20 January 2016

[viii] https://www.oaic.gov.au/privacy/australian-privacy-principles accessed on 20 January 2016

[ix] https://www.infrastructure.gov.au/sites/default/files/2014-112101-CLOUD-Consumer-factsheet.pdfaccessed on 20 January 2016

[x] https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance