Queensland Law Society

Choosing and using cloud services

A quick reference guide

October 2020

Cloud computing for law firms

Quick overview

- Firms – of any size – need a process to check cloud providers before using them. Even well known companies may have privacy policies that are not acceptable for client data.
- Staff need to be told – and reminded - that they cannot set up or use cloud accounts without these being approved.
- Policies of this kind get circumvented or ignored if the firm does not supply realistic alternatives, and all policies need to be explained and discussed.
- Assessment should cover privacy, security and how data is to be tracked and integrated with other firm systems.
- Larger firms should consider a structured risk management and assessment process for all cloud services. The Australian Cyber Security Centre has introduced a new uniform assessment guideline process (June 2020).
- Annexure A to this guide contains a cloud project checklist.

Ethical and practical considerations

Most small and medium law firms these days use at least some services which host or process client data in the cloud. Sometimes this was introduced as a structured program to retire on-premises servers, but often cloud adoption is product-by-product - perhaps without much advance reflection.

Whether it is a cloud-hosted practice management system, Office 365, accounting, video conferencing, email or mobile apps, at some point data entrusted to us by clients is likely to end up on a remote network.

There is nothing inherently less secure about cloud data providers and it is perfectly acceptable for law firms to use them. Only a very well maintained on-premises server is likely to be more secure than a professionally run data facility, and well implemented cloud use can help keep firm data in one location rather than saved to laptops, phones and USB drives.

However, we cannot simply assume that cloud vendors will adequately respect or protect our client's confidentiality. Part of our duty of competence extends to appropriate selection of third parties to perform subcontracted services.[1] The applicable standard is not strict liability, but reasonable endeavours expected of a competent practitioner given the resources available. For larger firms this will often require a structured due diligence process undertaken by a qualified information security professional. For a small firm, enquiries of sales agents and consideration of published privacy and security policies is prudent, even if there is no realistic capacity to test whether the provider actually implements what it claims. Sticking to "brand name" providers helps as well.

Many organisations do not have policies controlling the use of cloud services, and even those that do have such policies are still likely to have data in accounts set up in contravention of them.[2] Even if the contravening locations are fairly secure, if you don't have the password or can't easily integrate data into your usual document management system the data is not under adequate firm control. Even two and three person firms need an agreed position about which productivity and connectivity tools can be used and how. Like all information security policies, discussion and training are essential for them to work, and providing a reasonable alternative is usually far more effective than simply prohibiting all cloud-enabled services.

[1] This note is aimed at firms that are not regulated by the *Privacy Act 1988* (Cth), which sets out specific requirements in the National Privacy Principles.
[2] Surveys of "shadow IT" show that most organisations have data in unauthorised cloud locations – not just a few, but potentially hundreds of them. See Kenneth Corbin, 'CIOs vastly underestimate extent of shadow IT', *CIO Australia* (10 August 2015) <https://www.cio.com/article/2968281/cios-vastly-underestimate-extent-of-shadow-it.html>.

Part I: choosing a service provider

There are three elements to consider: *privacy*, *security* and *practicality*.

Privacy relates to the stated purposes for which the third party holders may use your client and firm data. Providers of free services will usually monetise their business by employing the data held, often by selling access for targeted advertising. Even where data is de-identified, such use may contravene the duties you owe to your clients. When several data sets are combined it is often possible to "re-identify" who the data relates to, and in any event clients would not expect the information they send to be handed over to third parties to be data-mined. Consequently, the standard for client data is fairly straightforward: no third party use or sharing of data except to permit service delivery or compliance with law is acceptable.

Given the number of "click through" terms of service we accept every day it is easy to get into the habit of not reading them, but in the case of your business data doing so is essential. While providers may attempt to obfuscate data monetisation, disclosure will usually be somewhere in the Terms of Service or EULA. Apps purchased directly from the Google Play or Apple stores or overseas may not comply with Australian laws and background research about their privacy reputation may be necessary.

Another element to privacy is data sovereignty. By definition, cloud data can be hosted anywhere. Ideally, you should receive a guarantee that data will be (primarily)[3] held in Australian data centres. Next best is Europe. US data management standards are also high, but the US government has wide access powers.

What to look for when assessing privacy

- **Payment.** There is no such thing as a free service – on the Internet or anywhere else. You either pay for a product or you *are* the product.[4]
- **Access and monetisation.** No third party access to data, no data sharing of any kind, even anonymously.
- **Location.** You should be told in which jurisdiction your data will be held.

Security relates to the systems the provider has in place to avoid data theft. While stated policies do not mean much if poorly implemented, the fact that the policies are there to begin with (as opposed to vague statements that "we use Military Grade Encryption" or "security is our top priority") are a positive sign.

How can a solicitor without an information security background assess the competence of an online provider? In short, we usually can't to any significant degree. If all your client data is to be entrusted to the provider it may be necessary to pay for a qualified person to investigate and supply a Cloud Security Assessment Report. This can be expensive. The higher security that can be expected of "brand name" providers like Microsoft might preclude the necessity for bespoke investigation, although the provider's best practice guidelines should be followed.[5] With luck, a cloud provider may have an audit report available.[6]

Such analysis may not fall within the skill set of your IT consultant, and never within their terms of service unless specifically contracted. It is therefore unreasonable to assume that they would

[3] Data location may be complex. The important question is where the bulk data uploaded by your clients will reside. Other data pertinent to your account, such as your own contact and billing information may be accessible offshore to facilitate billing, tech support and ancillary services.
[4] The one exception is a limited functionality license from a provider trying to interest you in their paid services. However, even in this case caution is required as free subscriptions may come with advertising and advertising is worth a lot more if directed at a targeted audience.
[5] Keep in mind that the service provider may not the same as the platform provider. For example, an accounting package may host data on Microsoft's Azure platform, but security is not Microsoft's responsibility under this arrangement.
[6] A new assessment standard format was released by Australia's ACSC in June 2020. Complete assessment by this standard may not be available: the checklist contains over 800 items, each one of which may take hours to answer and confirm.

undertake security assessment if their brief is simply to configure your network to use the new service.

What to look for when self-assessing security

- **Market reputation.** Security is expensive, and start-ups usually can't afford it. Fortunately, many reputable security researchers publish assessments of well-known cloud providers and considering a variety of these can be useful.[7]
- **Platform.** Most cloud providers will host data on a "brand name" platform (Commonly Amazon Web Services, Google Cloud Platform or Microsoft Azure). A small provider not using one of those platforms is suspect. Using one is a good start, but only part of the security comes from the platform. Don't let a sales person tell you that "our data is secure because it is hosted by Microsoft".
- **Certification.** Look for ISO 27001 (information security generally) and / or ISO 27017 (information security for cloud providers).
- **Authentication and sign on.** The most common way cloud data is compromised is a password being stolen. To minimise this risk, good password practices are essential, and if a cloud provider does not offer Multi Factor Authentication it should not be used.[8] See QLS resources on passwords and multi factor authentication here.
- **Encryption.** Encryption is a standard security measure and should apply to data both in transit and at rest. The encryption offered by the provider can be supplemented by services such as Boxcryptor, which allows you to encrypt all content before it is uploaded (this is especially useful for data storage and transfer systems such as Dropbox and Google Drive). Encryption is not a panacea, especially if user access controls are poor.

Practicality: commercial and other considerations

- **Pricing tiers.** Once you have built systems around using one provider it can be onerous to change. Always consider the price tier above what you need now to ensure the service will remain suitable if your business expands.
- **Seamless data integration.** The real benefits of cloud computing are achieved by interoperability. Services fragmented into multiple pockets that do not interact easily will never be as useful as a system that shares data seamlessly. Integrated systems may cost more up front, but the labour savings may more than offset a higher up-front cost. Connector services like Zapier are popular, but the cost has grown and it is extremely difficult to assess security where data is moving through multiple cloud systems.
- **Getting in.** Just because existing client data can be uploaded to a cloud service does not mean that this is cheap or easy to do safely. Before committing, find out what support is available and how much it will cost.
- **Getting out.** Is there a way to uplift data in bulk if you change providers? While limitations on the number of files that can be copied at once can enhance security, it can also make transition very difficult if you decide the service no longer suits your needs. Are there any costs? Will existing file structures be maintained? What formats are available? Are those formats available for all file transfers or is that limited?
- **Zombie accounts.** What will happen if you close the account? Will the data in it be deleted?[9] Will that be confirmed by the vendor?

Part II: using cloud services

Policy and Procedures. Even small firms need IT policies, albeit not especially complex ones. There are several main objectives:

---

[7] These may be published reviews or reports available for purchase. Online and automated assessment reports will be cheaper than a bespoke investigation, but assessment of smaller legal industry specific services may not be available.

[8] There are some acceptable alternatives to MFA, such as Single Sign On ("SSO") options (another trusted company such as Google is used as the authentication point) or passwords are replaced altogether.

[9] Be careful of the language here. Some providers will seek to hold onto the data and "anonymise" it. This may be described as "deactivation" or something similar. If there is no explicit promise of deletion this needs to be checked.

- Make sure people know not to use unapproved services
- Make sure you control what data goes in and out.

One of the most common problems with cloud accounts is that they are not controlled by the firm. If a long departed employee sets up a drop-box account this can be very challenging from a business continuity perspective, and makes it hard to comply with your record-keeping or disclosure obligations. Transfer of confidential information to a cloud account not controlled by the firm will be regarded as a data breach, potentially activating contractual and statutory obligations.

Annexure A to this guide contains two template policies: one for a small firm, one for a somewhat larger one. These may be downloaded and used but some customisation will be required.

Policies have little effect if staff do not apply them. A little effort bringing policies to the firm's attention and explaining why they are needed significantly increases compliance and your data safety. Some guidance to the change management aspects of deploying security software and policies can be found on the QLS website here.

User authentication. One of the single most important ways an organisation can protect critical data is to ensure that passwords are strong and secure**. All cloud services must be protected by Multi Factor Authentication** or a secure alternative[10] and your firm should have policies and training to ensure partners and staff use appropriate passwords. Please see the QLS website for template password policies and the guide to Multi Factor Authentication.

Initial data migration. Many of the more significant cloud related data security incidents came from a mistake in moving the data from legacy systems to the new one. Migrating large volumes of client data is best done by an expert.

Backups. Just because data is hosted in a well-protected cloud facility does not mean it is invulnerable or that you no longer need to back it up. Data encrypted on your network by malware will still be encrypted when uploaded to the cloud, and errors happen even in large providers.

Disclaimer: Services, providers and software referenced in this guide have not been assessed by QLS. The use of all such software and services involves risk and QLS recommends that you obtain qualified advice prior to implementing any IT solution.

QLS has resources and programs to assist members to take all of the Cybersecurity steps recommended in this guide, and more. Call the QLS Ethics and Practice Centre for free and confidential information on p. 3842 5843

Enquiries: David Bowles, Ethics Solicitor, QLS Ethics and Practice Centre

[10] There are other secure ways of managing identity, some of which avoid the need for passwords altogether. A "bare" password is never sufficient to protect client data. (See Tim Ferrill, 'The Best Identity Management Solutions for 2020', *PC* (28 December 2019) <https://au.pcmag.com/migrated-6173-onlinecloud-backup-services/37371/the-best-identity-management-solutions-for-2020>.

Simple cloud project checklist

The golden rule: perfect is the enemy of good. Plan enough then take action.

WHY?

- ☐ What are the business objectives? Have I reviewed objectives and required functionality with all the teams that will use the system?
- ☐ Can this objective be achieved using a service or software I already have? Is the existing system obsolete and becoming dangerous? If not, should we wait for a better solution if those available now are not ideal?
- ☐ Is the service available as part of a suite, allowing seamless integration? What is the extra cost?
- ☐ List the critical factors the service MUST have and the top few that would be nice to have.

HOW?

- ☐ Can we implement this using internal resources? Is there good guidance available? Is there a plan B for support?
- ☐ Are all the features we have been shown available without extra payment?
- ☐ Are all those features available without customization or special implementation?
- ☐ What is the minimum required implementation budget?
- ☐ Who will be on the project team? What are their roles? Have they cleared diary time?
- ☐ Can our existing system run side by side until the new one goes live? What is the plan if the new system falls over?

COMPLIANCE AND RISK

- ☐ How critical is this data? What are the consequences of it being stolen or unavailable?
- ☐ Is the supplier's privacy policy available? Is any data sharing permitted (even anonymous)?
- ☐ Will my data be hosted in Australia? Does the contract promise that?
- ☐ Is the supplier ISO Certified (ISO 27001 / ISO 2701)?
- ☐ Can the provider offer an independent third party security report? If not, can I obtain one at reasonable cost? (Larger firms will need to justify any decision not to obtain expert assessment).
- ☐ Is Multi Factor Authentication ("MFA") available? (See QLS MFA Guide for types and benefits).
- ☐ Is data encrypted at all points in the use chain? Can I add another level of encryption?
- ☐ Does the supplier back up the data? Can I do so and keep my own copy easily?
- ☐ What happens if I ask these questions? Do we get an answer or a link to a website?
- ☐ Is the supplier (not just the platform where data is hosted) an industry leading brand (Check Gartner.com, Tomsguide.com, Capterra and PC Mag).

POLICY AND PROCEDURES

- ☐ Are there procedures we need to follow that will minimise risk?
- ☐ Are those procedures reflected in firm policies? How is training in those policies and procedures delivered? (Hint: an email telling people to read a policy document is not training).

END OF LIFE

- ☐ How is data migrated from the service? What formats are available?
- ☐ Will data be deleted if we end our subscription? Will such deletion be confirmed?

Cloud policy: Informal (Small firm)

What are cloud services?

"Cloud" computing services are provided on the basis that data is not located on our system but on a remote network. They are extremely convenient but need to be used carefully.

Policy

Client and firm confidential data may only be saved to or transported by cloud accounts approved by <<name or function>>.

Examples of cloud service providers

Gmail / Hotmail, Snapchat, SMS Messaging, Dropbox, Google Drive & Google docs, Xero, Most mobile device apps, Zoom, Trello, One Note. Nb: This is not an exhaustive list.

Examples of contravention

- Emailing a letter / file to your personal Gmail account so you can work on it at home.
- Setting up a drop-box account to keep a copy of files you are working on or deliver a brief.
- Using a Google Docs form to make time entries from your mobile.

What is the problem with cloud services?

There are three issues:

(1) Some allow data to be shared for advertising purposes. This is not acceptable for confidential client data.

(2) Some do not have adequate security

(3) It can become very hard to maintain complete and accurate client records where information is spread between different accounts.

If you have a business need that our on-premises systems cannot meet, we will do our best to find an alternative that is acceptable.

Amnesty and rectification

If you have been using unauthorised cloud accounts, we understand that this may have been with good intentions, and provided you let us know during the amnesty period there is no problem with prior use. The amnesty period starts <<Date>> and ends <<Date>>.

Please let <<Name / function>> know and we will work out a process to get the data back onto our systems.

Consequences for contravention after the amnesty ends

Compliance with this policy is a condition of employment and partnership. Deliberate contravention may result in termination of either of those relationships. Voluntary disclosure is a significant factor when considering the severity of contravention.

Cloud Computing Policy (Mid-size firm)

What are cloud services?

"Cloud" computing services are provided on the basis that data is not located on the user's device but on a remote network. They are extremely convenient but need to be selected and used carefully. Many people use them in our daily lives and it seems natural to use them for work purposes also, but this is not acceptable without due diligence and approval.

Potential problems with unauthorised cloud services:

- **Privacy:** many cloud services allow advertisers to access information about user identification and data content. They say this is anonymised but often that process is not adequate. Some providers routinely share content with foreign law enforcement.
- **Security:** platform security may be inadequate and the process for getting data in/out may bypass firm security systems. Data removed from firm control to a cloud service may amount to a data breach in itself, triggering regulatory or contractual consequences.
- **Data integrity:** documents left in cloud storage may lead to client records being incomplete or misleading. Negligence claims or disciplinary prosecutions can arise.

Firm policy

Cloud services must **NOT** be used without express approval from <<function or department>>. Partners and staff may **NOT** create or use cloud based data storage, manipulation or exchange of firm-related communications or firm-owned data without such approval. This is necessary to protect the integrity and confidentiality of our data and comply with ethical and statutory obligations.

Our IT department remains committed to enabling employees to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby <<firm name>> can use cloud services without jeopardising firm data and computing resources.

Who does this apply to?

This policy applies to all staff (permanent or temporary).

This policy pertains to all external cloud services, eg cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded, but firm data may not be stored or transmitted using personal accounts.

If you are not sure whether a service is cloud-based or not, please contact the IT department.

Specifics

- Use of cloud computing services for work purposes must be formally authorised by <<function or department>>.
- For any cloud services that require users to agree to terms of service, (ie, all of them) such agreements must be reviewed and approved by <<function or department>>.
- The use of such services must comply with <<firm name's>> existing:
    - Acceptable Use Policy/Computer Usage Policy/Internet Usage Policy.
    - BYOD Policy.
- Employees must not share log-in credentials with co-workers. The IT department will keep a confidential document or password management system containing account information for business continuity purposes.

- The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by <<firm name>>.
- The <<function/department>> decides what data may or may not be stored in the Cloud. Conditions and processes may be mandated as part of that approval.
- Personal cloud service accounts may not be used for the storage, manipulation or exchange of client-related communications or firm-owned data.
- Personal cloud service accounts may not be accessed on firm owned equipment without approval.

Pre-approved cloud computing services

The services listed below are approved for <<firm name>> usage:

- <<services>>
- <<services>>
- <<services>>

NOTE: This policy may not be General Data Protection Regulation (GDPR) compliant.