Cloud computing is a general term to describe “a variety of different types of computing concepts that involve a large number of computers that are connected through a real-time communication network (typically the Internet).”

Cloud computing has great appeal for business and law firms for a number of reasons. Benefits include affordability (cloud based software programs can reduce IT complexity), accessibility (given many cloud computing applications include access from anywhere, an easy set-up, off-site work can save rent and travelling costs as well as facilitate joint working amongst the offices of multi-locations law firms) and, flexibility (users can access files stored on the cloud as long as there is an Internet connection from anywhere at any time).

Notwithstanding the benefits, consideration of the risks is necessary.

The Australian Government has released a policy for the Government’s use of cloud computing called the “Australian Government Policy and risk management guidelines for the processing and storage of Australian Government Information in outsourced or offshore ICT Arrangements.” It is available on the Protective Security Policy Framework website.

So what are the associated risks for the legal profession? Lawyers have a number of ethical considerations particularly regarding the data itself and access, contractual provisions for disclosure of confidential information to third parties including via the discovery process and, record keeping.

---

1 Wikipedia definition
2 http://www.protectivesecurity.gov.au
The following are some of the issues that need to be considered:

Off-site data attracts a high risk. Where will the data be stored? More often than not the cloud computing service providers are located overseas. Accordingly, consideration needs to be given to the relevant privacy and the security laws applicable to the data as the geographic location will dictate.

Loss, leakage or compromise of data needs to be factored in. Unauthorised parties may gain access to sensitive data. Inadvertent deletion or alteration of records without a backup of the original content may occur.

After the termination of a matter, will the relevant data be kept for an appropriate time?

Certainly questions that require answers also include the following:

- Where will users be located?
- Where will the data be processed?
- Where will the data be stored?
- Where is the disaster-recovery and back up site located?
- Where are the data subjects located?
- Where will support services be based, and will support have access to sensitive data?
- Will sub-contractors or outsourcing be utilised for any functions having access to sensitive data?
- Does the customer have the right to approve in advance any transfer of data to another state or country?
- Who will have access to the data and will there be different levels of access?
- Who will supervise the project and will there be monitoring and auditing of policies and procedures?³

Ultimately there are many risks with cloud computing and they need to be weighed up against the legal and safeguards as to whether the cloud is the appropriate storage place and if so, heed, it is necessary to proceed with caution.

For any queries about this or other Risk Management Services offered by Law Claims, please contact the PII Risk Manager, Gianna Di Stefano on 8410 7677 or gdistefano@lawguard.com.au.