The Cloud – Guidelines for Solicitors

A bullet point document to generate discussion in an organisation planning to use, or increase use of, the Cloud.

Tim Newton – Managing Director

Business & General Consulting Ltd

May 2014

Contents

Introduction

The Cloud makes it simple to share documents with colleagues and clients. Given the sensitivity and confidentiality of Client data, legal organisations have a duty of care to protect this information.

There are any number of articles written which attempt to advise users on the Cloud and the "best" applications available. However, most of these articles are targeted at the Consumer user, not the Business user, and certainly not the Legal user. This document helps to address that shortfall during initial discussions and planning. It highlights areas which ought to be considered before deciding to move documentation to the Cloud, whether for storage purposes only (backup) or for collaboration (sharing information with individuals/teams both internal and external).

Terminology

In this document, **"Provider"** refers to the Cloud Service Provider, the company or organisation providing the environment where the data is to be stored. **"Customer"** refers to the owner of the data, the customer of the Cloud Service Provider. To avoid ambiguity, the term **"Client"** means the Customer's own client/customer.

The Cloud and Contractual Considerations.

Legal Issues

SRA Recommendations.

In the UK, the Solicitors Regulation Authority have produced a guidelines for Solicitors with some excellent considerations – which is readily available at http://www.scl.org/site.aspx?i=ne34338

The guide includes a useful checklist. The recommendations for best practice for due diligence includes:

- Taking references from other companies using the proposed provider
- Checking service level agreements carefully to ensure that the proposed service can offer at least full Safe Harbour compliance if data is stored outside the EEA
- Checking that the provider can offer audited information security that at a minimum is compliant with ISO27001 2005
- Checking that the provider can offer a level of guaranteed uptime and continuity protection that is acceptable to the firm
- Ensuring, where staff will be working on the move, that they have properly secured communication channels to protect security
- Ensuring that their contract with the provider includes the requirements of Outcome 7.10 of the SRA Code of Conduct.
- Using a private cloud, or private area of a hybrid cloud, for client confidential material
- Using software to automatically encrypt documents at the law firm's end, using security keys that are not known to the provider
- Using only providers that are based in EEA countries or countries offering equivalent or greater data protection laws, and that can guarantee that data will not be held in jurisdictions that do not offer such protections.

The SRA guide is by no means against the use of cloud computing, recognising that one of its major advantages is that it enables mobile working without the need to carry data around on laptops or datasticks, which are the main risks for data loss. Cloud document sharing also reduces the cost of Large Letter Post Office fees which rise at a regular rate.

UK/EU regulations.

UK law with regard to the Cloud is generally driven by EU regulations. At the time of writing, the two important pieces of EU documentation are :

- 1995 EU Data Protection Directive and
- 2002 ePrivacy Directive as amended 2009

These laws contain components of security which must be adopted by subcontractors. Areas to be aware of include :

- There is a contractual obligation to protect the personal information of Clients:
  - To ensure data isn't used for secondary purposes
  - To ensure data is not disclosed to third-parties.

- Contract wording with the Cloud Provider should reflect the promises and commitments made in the Client contracts.

In summary, any contract with a Cloud Provider should ensure that data usage and privacy is of the same extent as it would be in a non-Cloud relationship.

Contract Considerations

Due Diligence

An organisation will evaluate its' own needs, restrictions and practices to identify the compliance requirements. This is not a "one solution fits all" review. Each business area or business transaction needs to be analysed to determine answers to (for example),

- Does the business model allow for Cloud use for this business type
- Under what conditions should the Cloud be used
- Should control of this transaction really be relinquished to the Cloud Provider
- Is the data use restricted by law or other security concerns
- Will the Cloud Provider be able to fulfil the Customer's obligation to protect its' data assets.
- Is after-sales Support responsive and effective. Ask for references from existing users and check social media (Twitter etc.) for comments on Support.

Contract with Cloud Provider – Considerations.

Most Cloud Providers contracts consist of a "click here to confirm that you accept our terms and conditions" – an off-the-shelf contract with little or no room for negotiation or clause amendment. If so:

- Balance the risks of the contract with the benefits and cost savings of the Cloud Provider.
- Check the small print – beware of terms such as "a worldwide license to use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute such content."
- Check the level of Support – what response time is guaranteed
- Given the nature of US surveillance laws, your data should be stored on UK or EU servers only.
- Consider whether the data should be placed into the Cloud given the contract terms
- Consider another Provider

If negotiation is possible:

- The contract terms should include needs and obligations of both parties during the contract period.
- At the end of the contract period, it should be clear what happens with the stored data, how it is returned to the Customer and how it is deleted from the Cloud, including backup copies and metadata.

Cloud Specific Issues

The Cloud is not a static environment. Over a period of time there will be changes – some necessary (Security updates from Operating System providers, anti-Virus updates etc) and others optional

(switching of existing data to a new server, new technology adoption, new compliance requirements etc). During these changes, it is important that :

- The Cloud Provider and the Customer ensure that their own compliance needs are met
- The required security measures/policies are being used. This is best done by ongoing monitoring, testing and evaluation of the services.

Special note for Solicitors – Discovery

One of the requirements of discovery is that a litigant must provide all documents pertaining to a case. Not only favourable documents to the case but all documents which are of interest to the opposing litigant. Over the years, there have been a number of recent news reports where documents have been deleted, lost or modified. As a result, in the USA, the regulations now cover electronically stored information ("ESA)". The following points are general to this area and should be noted:

- Cloud Service providers and their customers must plan how to identify all documents pertaining to a case. Once a Customer determines that data is relevant and needs to be preserved, there may need to be discussions with the Provider to ensure this is done in a reasonable fashion.
- In some cases, where data stored in the Cloud is highly relevant to a case, the Cloud provider may receive a subpoena or similar discovery process directly.
- A Customer may not have the administrative rights to search access the data hosted in the Cloud. This could result in additional costs to find and retrieve this information. Collection from the Cloud may prove more time-consuming and costly than retrieving data from the Customers own servers would be.
- Information must be preserved during a case. This requires the Customer (and therefore the Cloud Provider) to have agreements in place to prevent the destruction or modification of data.
- Preservation can require huge volumes of data stored over extensive periods. The Customer should be aware of the costs of this, and also check the contractual terms should the storage outlast the terms of the SLA or Cloud Provider contract.
- Direct access to a responding party's internal IT system is not generally favoured, but possible. However in a Cloud environment, the hardware and facilities may well be outside of the control or custody of the Customer.

Governance/Compliance

General Considerations on Compliance

Technology in the Cloud is subject to ongoing and changing policies and regulations. IT Governance is necessary to deal with these requirements. This is a complex and detailed subject area, best handled via professional advice, however the key points to remember are :-

- Review each area proposed for the Cloud and determine if moving to the Cloud would impact existing compliance or policies.
- Agree on how to collect compliance evidence via Activity Reports, Incident reports and response times etc. These can be covered within the SLA agreement but should be considered prior to moving any data to the Cloud.
- Personal Identification Information is subject to a host of regulations that vary by country. Since the Cloud is geographically diverse, data may be stored in many locations or across multiple data centres. This has legal ramifications depending on where the data is stored.
- Geographic location will become a priority where a Client requests or policies demand that data is only held within one geographic location or region (e.g. US only, EU only etc). The Ensure the Provider does not transmit data outside the required location.
- Be aware of the nature of surveillance laws if data is stored or transmitted via some countries (e.g USA).
- For each document, you should be able to see who changed what and when and be able to segregate readers from editors/authors.
- Classify information into at least high level categories such as “Public”, “Regulated” and “Highly Confidential”. For each category , policies will be required for
    1. What activities are permitted at each category level
    2. Where data may be geographically located for each category level
    3. Which types of employees are allowed access to which cateogries
    4. Ownership – who is ultimately responsible for the information at each level.

Data Security Compliance

Many companies report that employees often move sensitive data to the Cloud without the approval or notification of IT or Management.

- Access controls and encryption are required to prevent this.
- IT teams can implement URL filters and blocking to stop access to unauthorised public Cloud services.

Protecting data in the Cloud

It is important to protect the data in transit to/from and while stored in, the Cloud. There are 3 options available, of which the SRA only recommends Client-side encryption:

- Client Side Encryption. Data is encrypted before being sent across to the network to the Cloud provider. Keys and/or are held by the Customer not by the Provider. This dramatically reduces the effect of any data-leakage from the Cloud Provider’s system. Further, it stops

Cloud employees or hackers from viewing, editing or forwarding the data to unknown recipients.

Portability Issues

A Customer needs to understand how differences between Providers may affect the ability to switch Provider if required :-

- Different SLA's. Compare the SLAs of the existing and proposed providers to ensure requirements will be met.
- Architecture – different platform architectures may limit the ability to port data to the new provider.
- Security
    1. Authentication across systems must be maintained
    2. Encryption keys should be ported across or at least maintained and escrowed locally
    3. Metadata will also require porting and deleting. This is often overlooked – Metadata is important in the Cloud as it moves with the document. The contract with the provider should ensure that, when moving files to a new provider or environment, all existing copies of the metadata are destroyed to prevent this information from remaining behind on the old system.

Summary

This document should drive internal discussion and review prior to relocating information to the Cloud. The choices of product and service provider are ever increasing – and it is important that any Customer checks at the outset, and continues to check during, the terms of the contract that the relevant security and safety policies are in place and are being used.

Security Consultants have in-depth knowledge of both the requirements and detailed history of previous failures. Using a consultant will help to identify and minimise the risks involved when storing information in the Cloud. Business & General Consulting Ltd have over 15 years experience of business over the Web and 2 years experience of advising and planning secure cloud implementations.

For data storage, Tresorit fulfils the software security requirements for data uploaded to the Cloud and is recommended at http://legalservicereviewblog.com/2014/01/new-must-apps-lawyers/

* * *

For further information contact Tim Newton on 02392 990168 or tim.newton@tresorit.com

