Law Society of Scotland

Guide to cloud computing

In association with

Clio

Contents

Benefits and risks

Cloud computing – the use of computing resources that are not on your premises – can bring many advantages. However, it also presents some risks and challenges. It is important to understand cloud computing – and decide if it is right for you.

The benefits of cloud computing:

- Cost savings – reduced upfront investment in physical products and infrastructure, such as servers, storage and expensive applications
- Ease of use – can be accessed any time and from any location
- Efficiency – can bring improvements in workflow, automation and collaboration
- Flexibility

Potential risks or challenges:

- The overall cost of cloud computing – subscription, licences, maintaining service – can exceed a traditional on-premise setup and should be properly considered
- Increased management will be needed as cloud computing is integrated into existing services and configured to your firm's requirements
- Staff training and education will be required

This guidance looks at how to find the service that is right for you, while also considering data, security and other issues.


if(parameters.Contains(
hql +=

Getting started

Understanding the cloud marketplace

It is easy to get started with cloud computing – but you should still think strategically about making the move. For instance, your new cloud services will need to interact with your existing IT systems, which may involve a complex mix of internally developed applications and third-party software. Any move to the cloud will involve a certain amount of disentangling. A sensible starting point is to simplify your existing IT system to establish what works well in-house and what would benefit from being moved to the cloud.

Private cloud v public cloud

The majority of cloud computing services are now delivered through what is known as the public cloud. These services are offered on a 'one-to-many' or 'utility' basis. This means that the standard functionality of the service is offered to all, although some element of customisation or configuration for individual needs can still take place. For example, using a public cloud-based email system would allow you to configure mailbox settings and dictate who has permission to access the service and from which devices, but would not allow you to demand changes to the supplier's security policy. Public cloud services typically share hardware and software between multiple clients of the provider, with only software-based security controls in place to make sure that one client cannot access another's data. A key factor with public cloud services is that the terms of the contract tend to be fairly fixed. Provided you are satisfied with the functionality, compliance and security arrangements on offer, it is perfectly possible to run the majority, or indeed all, aspects of a legal practice using the public cloud, including email, document production, practice management, storage and networks.

By contrast, private cloud services are tailored more precisely to the needs of the customer. For example, it is usual for private clouds to be run on separate hardware, which adds an additional layer of physical security. As with more traditional IT procurement, fully negotiated agreements are more likely to be put in place to meet specific customer needs, albeit such a bespoke arrangement is likely to come with a commensurate price tag. Larger law firms are likely to make use of a hybrid cloud offering, for example, using an on-premises private cloud to host sensitive data and critical workloads and a third-party public cloud provider for less critical resources. Most smaller legal firms are likely to use public cloud services, possibly with some element of bespoke work to integrate with other practice systems.

Client considerations

A significant proportion of the data that a law firm may look to place in the cloud will relate to clients. Clients will have expectations that this data is held securely and safely, and in accordance with regulatory requirements and any engagement terms.

Unless specifically prohibited by the engagement letter, no specific client consent is required to make use of cloud providers where the law firm is acting as a data controller. However, if the personal data is going to be processed by the cloud provider outside the European Economic Area (EEA), it will be necessary for the law firm to satisfy itself that the security arrangements proposed are compliant with the General Data Protection Regulation (GDPR), and that the GDPR requirements relating to international transfers of personal data are met. Where the law firm is acting as a data processor, it will require the client's specific consent to the use of cloud providers, which can be given either in the engagement terms themselves, or by separate written instructions.

Questions to ask providers

Cloud computing providers range from large, international organisations to local companies and others specialising on the legal or professional services market. It is important to ask some key questions to ensure a potential provider meets your service delivery, security and compliance requirements. Questions to ask include:

- **What commitments around availability and performance of the services are being given?**
- **Where will my data be held?**
- **How easily can I get data back, both during and at the end of the service?**
- **What backup arrangements are being offered if the service goes down?**
- **What security arrangements are in place?**
- **If using a shared rack in a shared data centre, what would happen to my data if another customer's server on my shared rack was seized, perhaps by a regulator for investigatory purposes?**

A cloud solution hosted on a dedicated server will come at a premium but should ensure a greater degree of security and control of your data and systems.

Key contract provisions

Services provided

Service description

Service descriptions in cloud contract agreements can be vague – it is important that they are clearly specified. Key points when agreeing a contract include:

- Ensure there is a service description that is precise enough to be relied on – but not so technical that it is difficult to understand. While the marketing and technical documents can be useful guides, neither is likely to be pitched at the correct level to form the actual service description.
- Check whether the service is being offered on a 'reasonable endeavours' basis only, or something more concrete.
- Check whether the supplier can change the services without your consent or without sufficient notice – and whether this could result in you losing key functionality, or the cloud service no longer working with other aspects of your IT system.
- Consider whether you need a period of testing or acceptance before paying the charges in full. Not all cloud services are ready 'out of the box' – it is important to check compatibility with your other systems at the outset.

Change in business requirements

Be mindful of your business plan when you place the initial order for your cloud service: are you intending to expand your business? Think further than your immediate business requirements.

One advantage of cloud services is the flexibility to change the level of service provided as required. Any professional cloud supplier should ask if you have any expansion plans to enable them to design the best fit for your business – in the short, medium and long term. In some cases, there may be little difference in cost.

Always ask a cloud supplier the costs of adding more applications, services, users and storage to ensure that these are not disproportionate or would obstruct expansion. Also, be mindful of your own protocols and procedures for increasing services. Due to ease of use, there is a risk that you consume more of the cloud service than intended, which can mean higher than anticipated bills. Ensure that the contract makes it clear who has authority to instruct increases in usage and how you will be notified if services are being used above a certain level.

Always ask if there are any additional charges for configuration, project management, implementation and support. Likewise, find out if there are charges or notice periods for decreasing your service requirements.

Licences

The responsibility for software licences can be a source of potential confusion with cloud computing.

Where the service involves the provision of software or applications (known as 'software as a service'), the provider should arrange all necessary usage permissions.

However, if the service you are receiving involves the provision of a software platform or infrastructure, you will be responsible for ensuring that it is properly licensed. Make sure you are clear whether it is the provider's responsibility to arrange and manage any requisite software licences together with the payment of any associated fees, or whether this falls on you as the customer.

Key contract provisions

Service levels

The service levels, which are often set out in a separate service level agreement (SLA) schedule, will cover:

- The availability and performance standards to which the services are to be provided
- The remedies available if the service fails to meet the terms of the SLA
- Particular areas of the SLA to look out for include system availability, support and maintenance, and remedies for unscheduled downtime.

System availability

The time a computer system is operating is called uptime. It is usually shown as a percentage. Care should be taken in understanding how this percentage is calculated because it will allow for service outages when your data is not available. For example, if a provider specifies an outage as being anything of 30 minutes or more, and the service is not functional for 29 minutes, uptime may still be 100%. You should check whether these outages will be announced in advance and whether they will occur outside of your normal working hours.

The definition of 'up' is also important. Your cloud system may be 'up' according to your SLA even if a number of features are unresponsive, provided that core systems are available. Ultimately, your availability figure should mirror the time you actually have access to a fully functional system (or, at least, functional in all critical respects).

Ask your provider for evidence of its history of downtime and the measures that have been taken to prevent similar incidents in future. You could also contact reference customers of the cloud provider.

Support and maintenance

Given the nature of the cloud service (and certainly public cloud), support and maintenance should be included as part of the standard pricing model, since this will be required to keep the service operational. However, it may be that only basic support is included in your package, with premium support available at an extra cost. Pay particular attention to helpdesk opening hours, as well as response times and procedures. The initial helpdesk response may simply log the problem with a further call back to provide substantive support.

Like most modern IT systems, cloud arrangements depend on internet availability. Also, your IT equipment will need to be of a certain technical specification to access the cloud service. You should ask whether your provider will offer advice on, and support with, checking the necessary equipment and internet connection required for optimum cloud system performance. Your provider may also advise on contingency plans for internet outages.

Remedies

Your provider should give a clear explanation of the remedies for unscheduled downtime. Key issues are:

- Will you automatically receive service credits (in other words, a reduction in charges) in the event of failure?
- If so, are these set at a meaningful level?
- Is any further compensation available in the event of serious outages?

Business continuity and disaster recovery

Given that using cloud services effectively involves ceding control over aspects of your computing system, failure to consider business continuity and disaster recovery (BC/DR) could have a major impact on your business. This is particularly important if client data or crucial business functionality is moved to the cloud.

You should review the provider's BC/DR plan and ensure it is robust and comprehensive, and perhaps also that it is regularly updated and tested.

Your own BC/DR plan should address other factors that could cause you to lose access to your system, such as failure of your internet connection or a power cut. As part of BC/DR planning, to ensure there is no single point of failure, you should regularly test, and consider having fallbacks for, key resources, such as your internet service.

Upgrade path and compatibility

In establishing at the outset what is included in your subscription and what will incur further cost, you ask about upgrades to the service. Will you get upgrades automatically and, if so, how frequently? While frequent upgrades for security or functionality sound attractive, you should consider the compatibility of the cloud solution with your other IT systems. For example, if you are using the cloud for email, does this integrate with your document storage system, and how will upgrades affect this compatibility?

Security

In using a cloud computing system, you will give the supplier control over a number of areas that could impact on the security of your data.

The contract should spell out the security provided to ensure compliance with best practice and any applicable data and security regulations. This is often done by referring to the provider's IT security policy, which may make reference to international standards such as ISO 27001/ISO 27017. Bear in mind that data stored on a cloud platform could be lost through a malicious attack or a data wipe by the service provider. Always carefully review your provider's backup procedures as they relate to physical storage locations, physical access, and physical disasters and ensure that you have, if required, an independent recovery plan in place.

Your provider should also give assurances about the technical specifications and security of the data centre storing your data. There are various industry standards that can be used to check the quality and facilities of the data centre, including issues such as staff vetting.

Furthermore, your cloud provider should undertake to audit the facilities of its data centre at least annually. But do consider the true value of any audit findings produced by a provider. For example, will an audit report for a service provider (who may have shared cloud premises all over the globe) provide enough detail on the specific data centre where your server will be held, and perhaps even the specific area of the premises where your server sits?

Cloud security also depends, to a large extent, on the measures your firm takes. For example, your staff should use strong passwords and two-factor authentication. You should ask your provider to adjust settings so the use of strong passwords by staff is mandatory, there is an automated routine for passwords to be updated and the strength of user passwords is audited.

Data issues

Location of data

It is a common misconception that it is not possible to identify the physical location of data on the cloud; any reputable cloud provider will be able to give you that information.

The General Data Protection Regulation, requirements that come into effect in May 2018 to ensure proper procedures for processing and storing personal data in the European Union, places conditions on the transfer of personal data to third countries (i.e. those outside the EEA). It is recommended that you give consideration to requiring your cloud computing provider to store your data within the EEA, since this will greatly simplify the process and reduce the risk of breaches of GDPR.

Also, be sure to identify where data would be transferred to for backup, maintenance or disaster recovery purposes; your protections in the EEA would be undermined if data was accessed from, or transferred to, a non-EEA country in the event of an outage or force majeure event.

Access to data

You should ensure that your supplier offers a practical method of moving your data back to your premises or to another provider on demand. You should ensure that:

- There is a clear procedure – with firm timelines – for the return of data in the event you cannot obtain the data yourself
- There is an obligation on the supplier to make available/return the data in a usable format
- The supplier does not delete data on termination of the services without giving you a reasonable opportunity to recover the data.

Bear in mind that a solicitor has a responsibility to provide certain data to the Law Society and Scottish Legal Complaints Commission on request, and failure to do so could be a conduct issue. You may also be required to provide data in response to other legal requests, for example, subject access requests and repossession requests, or from HM Revenue & Customs, lenders under panel appointment arrangements and law enforcers. Your contract should therefore provide for the return of your data on demand, in a readable and understandable form, even if your firm is in breach of the terms it has in place with the provider, or if your firm is in a dispute (for example, regarding charges).

Retention of data

When data is deleted it is rarely removed entirely from the underlying storage media unless some additional steps are taken. In addition, a cloud provider is likely to have multiple copies of data stored in multiple locations to provide a more reliable service. This may include backup tapes or other media not directly connected to the cloud. Copies of personal data stored in a cloud service may also be stored in other forms, such as index structures.

You should therefore consider the provider's data retention policy. How, for example, will the provider's retention policy protect you and allow recovery for, say, an accidentally deleted email that contains important client information? In addition to regulatory requirements to retain data, and any undertakings that you may have given in the course of business to retain access to data and files, you must also consider proper disposal of data once these agreed time periods have expired. Ad-hoc disposal requirements should also be considered (particularly in the context of GDPR and the right to be forgotten, see the next page).

Backing up data

Depending on the service and the answers to your diligence questions, you may wish to consider regularly backing up the data held in the cloud and storing it locally. This will have technical and cost implications, but reduces the risk of being denied access to your data and makes the transfer to another supplier more straightforward. If you do hold a backup locally, you should check regularly that it is working correctly by creating a test file, deleting it and restoring it from your backup.

You should also check your contract for the frequency the cloud provider will back up your data to a separate site. You should be aware of any period of time where your data will not be backed up and will therefore be 'lost' should the cloud system fail.

Ownership and rights in data

Your cloud provider should give assurance that your information will be treated as confidential and not used or disclosed to third parties. In terms of intellectual property, you should retain full ownership of the data stored on your provider's system and have an explicit right to get your data back on demand. Also consider any intellectual property created during provision of the cloud service, which may be particularly relevant where interfaces are created between a cloud provider's systems and your applications. These would be valuable from a business continuity perspective if you were to look for a new provider or bring services back in-house. You should look to retain ownership (or broad usage rights) in those interfaces if possible. As regards usage rights in the data, please see the section over the page on GDPR.

Data issues

Audit and independent certification

You should ascertain your provider's willingness to be subjected to audits by independent security certification authorities. Some providers advertise certification summaries on their data quality and data security.

A number of industry self-certification schemes exist but it is not yet clear which represent a true 'gold standard' so they should be treated with appropriate care when selecting cloud providers.

Data protection and GDPR

Given the central role that the transfer of data plays in cloud services, the treatment of data protection compliance must be considered. Generally, cloud providers are keen to emphasise that they will act only as data processors. With the implementation of GDPR, obligations will be placed directly on data processors for the first time. Any person 'who has suffered material or non-material damage' as a result of an infringement of the GDPR has the right to claim compensation from either your firm (as the controller) or the service provider (as a data processor). Accordingly, cloud service providers may begin to seek their own warranties from you that adequate procedures are in place for data held in the cloud.

In terms of the cloud agreement itself, the key points are set out in the GDPR and include the following:

- Be sure that the supplier's role as a data processor is clear, and that the supplier does not have the right to use any of the data as data controller for its own purposes
- Ensure that the supplier only processes the data in accordance with your documented instructions
- Ensure that anyone who has access to the data is subject to confidentiality obligations (including the data processor's staff)
- The supplier must agree to assist you with relation to data subject rights as set out in the GDPR (including the right to be forgotten, the right to data portability and the right to restrict processing), otherwise you could find yourself unable to comply with these requirements
- The supplier must seek your consent to the use of any sub-contractors it engages that will process your data
- The supplier must have adequate security arrangements in place and a mechanism to notify you of breaches, including in enough time to allow you to notify regulators or data subjects within the legal time limits (See page 13 for more information).

You should also consider the effects of data protection impact assessments. Previously, such assessments were regarded as a matter of good practice but, under GDPR, they will be mandatory for any high-risk processing. You should ensure that the service provider undertakes to offer assistance to complete your assessments and, where necessary, engages in any consultations required with the Information Commissioner's Office.

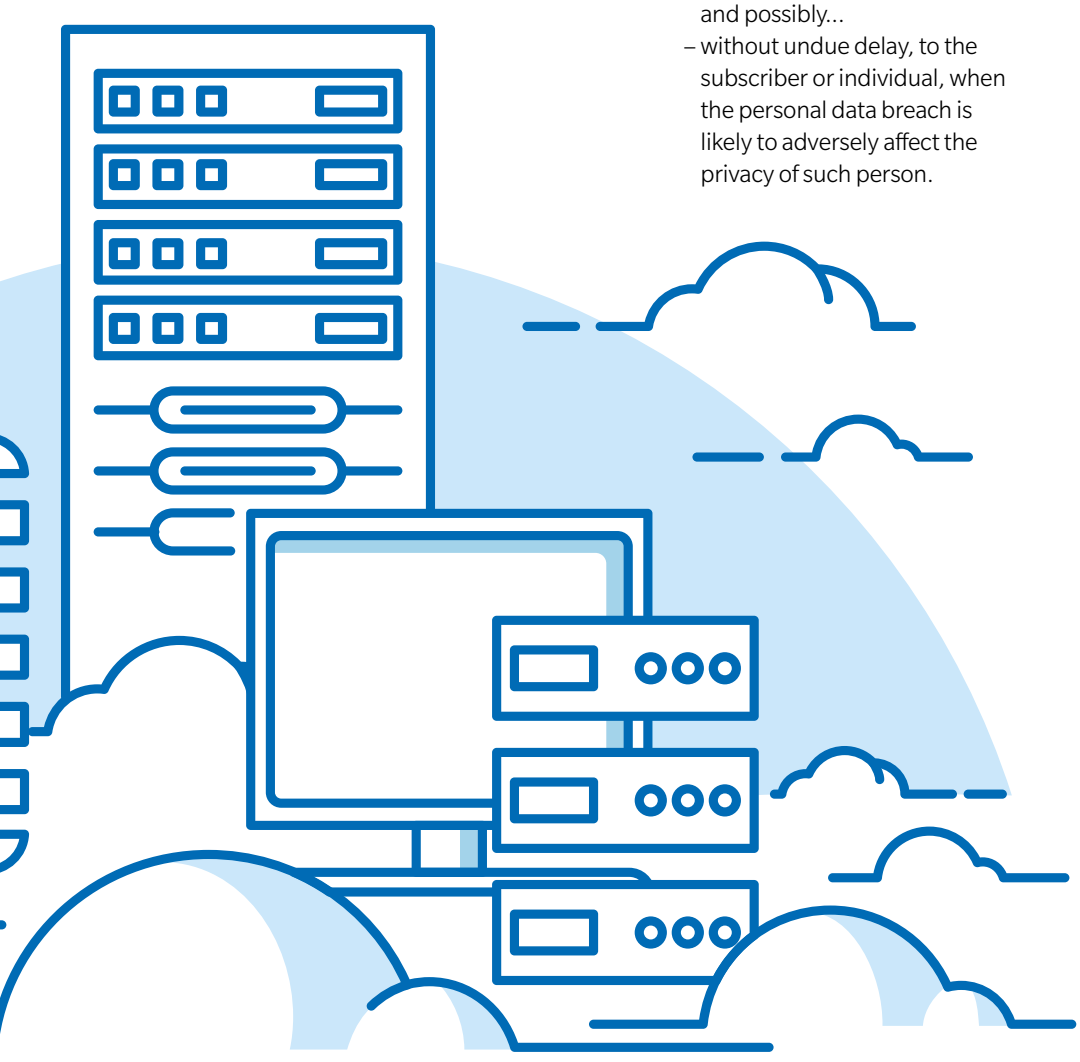
Under GDPR, the provider will have a responsibility to understand and keep an inventory of the data they are processing. In addition, the contract itself must set out in specific detail the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. This may lead to more debate about the allocation of risks and require greater due diligence before a contract is agreed.

Breach notification

The so-called e-Privacy Directive currently provides breach notification obligations for the providers of an electronic communications service, such as cloud service providers. This means that your service provider should:

- Inform subscribers about the risk of a breach of the security of the network, and in certain cases of the possible remedies;
- Notify a personal data breach:
  - within 24 hours after detection (where feasible), to the competent national authority; and possibly...
  - without undue delay, to the subscriber or individual, when the personal data breach is likely to adversely affect the privacy of such person.

GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. Therefore, in the event of a notifiable breach involving your client data, this may have to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. As such, you should ensure your supplier has a duty to notify you as soon as they become aware of any breach.



Other issues

Supply chain

It is important to be aware of sub-contracting carried out by your provider as this could affect the location of your data and your access rights. If you are unsure or not able to be specific about who holds your data and where they are, it could also create issues under GDPR or other regulations.

Suspension and termination rights and exit assistance

Cloud contracts often give the provider the right to suspend or terminate in the event of a breach of terms of use by the customer. This needs to be very carefully considered, as agreeing to such terms could result in a loss of a critical service.

Irrespective of how termination is effected, you should ensure that you have a suitable run-off period at the end of the contract. This will provide you with a period of continuity until you set up a new system, even if you breach the contract, and time to recover your data.

Further information

This guide was produced by members of the Society's Technology and Law Committee.
For more information, please contact **professionalpractice@lawscot.org.uk**
Tel **0131 226 8896**

Our sponsor

Clio

Clio is the most comprehensive cloud-based practice management platform for the legal industry and has been offering European legal practitioners a forward-thinking, easy-to-use solution to running and managing every element of a firm since 2013.

With the help of the cloud, Clio customers have regained eight hours of billable time. With a world-class team and a focus on their customers, Clio continuously creates innovative solutions. Clio employs over 240 individuals with a rapidly growing customer base spanning 90 countries and has been recognised by Deloitte on both the Fast 50 and the Fast 500 lists.

clio.com

In association with

Clio

Law Society of Scotland

The Law Society of Scotland
Atria One
144 Morrison Street
Edinburgh
EH3 8EX
T:+44(0) 131 226 7411
F:+44(0) 131 225 2934

www.lawscot.org.uk