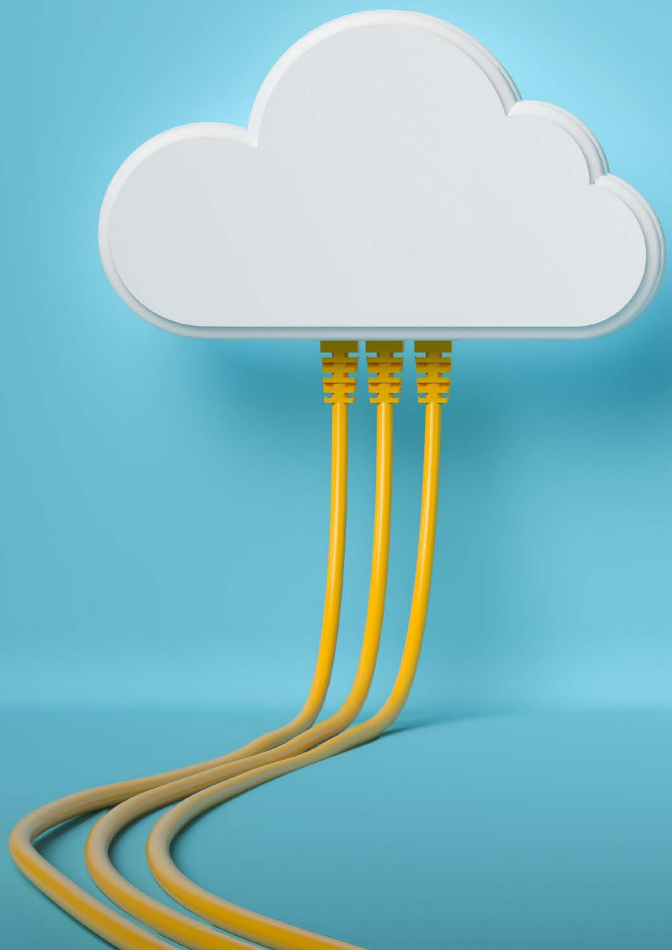
Law Society of Scotland

Guide to Cloud Computing



In partnership with

Clio®

Contents

Cloud computing involves the provision of pooled, centralised computing resources on-demand to customers via the internet. Most of us will be familiar with some form of cloud computing service, for example, email services accessed via a web browser.

Many organisations already use cloud computing to some extent, for example, software programs accessed online (previously, these were physically installed on the organisation's systems) or the use of remote infrastructure where an organisation uses a third-party data centre to store files and data.

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

Benefits and risks

Cloud computing can bring many advantages. However, it also presents some risks and challenges. It is important to understand cloud computing when determining which products are right for your organisation, and how best to implement them.

The benefits:

- Cost savings – reduced upfront investment in physical products and infrastructure, such as servers and storage
- Resource savings – your organisation's IT team can be freed up to work on other projects
- Ease of use – can be accessed any time and from any location (particularly beneficial with the adoption of hybrid working)
- Speed of deployment – can be quicker and easier to get up and running than a solution that needs to be installed on your own systems
- Efficiency/competitive edge – can bring improvements in workflow, automation and collaboration. Certain service offerings will have a higher availability offered by the supplier when deployed to the cloud rather than on-premises
- Quality - systems developed by specialist cloud providers can be better than their in-house developed equivalents by an organisation with fewer resources
- Future developments – cloud products are often more likely to be improved by the provider over time, implementing technical and practical enhancements that could be prohibitively expensive for a single organisation to implement
- Flexibility – can often be quickly scaled up (or down) to reflect the changing needs of your organisation
- Security – in the case of more sophisticated cloud products, it can be the case that the provider has greater expertise and investment in IT security than a single organisation with more limited resources – this can reduce the practical likelihood of a security breach
- Accounting / tax treatment – as a 'pay as you go' model, cloud subscription payments may be accounted for as an operational expense rather than the capital expense incurred when making more traditional on-premise IT investments

Potential risks or challenges:

- The overall cost of cloud computing – subscriptions and maintaining service needs to be considered across the longer term where costs could exceed a traditional on-premise setup
- Increased management will be needed as cloud computing is integrated into existing services and configured to your organisation's requirements
- Staff training and education will be required and IT policies may require to be updated
- Ill-suited products – a wide range of cloud products are available to meet varying needs, but they may not all be suitable for your organisation. For example, cloud document storage products will vary in terms of their cost, and (often proportionately) also their reliability, security and confidentiality assurances – using a free product to store confidential business information will likely create significant confidentiality, data protection and security risks. Cloud products require to be selected with the mitigation of these risks in mind
- Technical – cloud products might create inter-operability issues. One cloud product might use a specific format for the data stored within it that is not the same as another cloud product that it needs to communicate with. It is necessary to ensure that the data format used works with your other systems both now and in the future
- Downtime – using a cloud product rather than an in-house developed product will leave you relying on the supplier to fix any issues that cause downtime. You will not be in control of this and therefore there is a risk that issues are not resolved as fast as you would like or be able to do with your own product
- Supplier lock-in – like any third-party relationship, you may find yourself overly dependent on one or a small number of cloud providers. You should ensure you have given thought to a fallback option so that you are not overly exposed to future cost increases or service issues
- Risk of provider failure/insolvency – if the cloud provider has financial difficulties and goes insolvent, there is a risk to continuity of the service and/or access to your/your clients' data. This could occur, for example, if the cloud provider has its own contract with their provider of hosting services terminated for non-payment. Therefore, you should do your homework on the financial standing of the cloud provider and, where possible, monitor that on an ongoing basis. For provision of critical services, you may even wish to investigate cloud escrow services, which provides a mechanism to have another provider take over the cloud environment if your original cloud provider became insolvent

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, data migration and decommissioning of existing systems. 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 delivered through what is known as the public cloud. These services are offered on a 'one-to-many' basis. This means that the standard functionality of the service is offered to all, although some elements of 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 typically 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 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 infrastructure, which adds an additional layer of physical security. As with more traditional IT procurement, more fully negotiated agreements are more likely to be put in place for private cloud offerings to meet specific customer needs, albeit such a bespoke arrangement is likely to come with a commensurate price tag.

As a balance between the two offerings, the hybrid cloud has emerged - an infrastructure that includes links between public and private clouds so that it appears as a single environment to users - while the component entities remain distinct. Larger organisations are likely to make use of a hybrid cloud offering, for example, using a private cloud to host sensitive data and critical workloads and a public cloud for less critical resources. Most smaller organisations are likely to use public cloud services, as this can lead to an easier (and quicker) implementation with standardised upgrade schedules and a lower overall cost.

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 as the law firm will generally be acting as a data controller[1]. However, if the personal data is going to be processed by the cloud provider outside the United Kingdom and/or European Economic Area (EEA), it will be necessary for the law firm to satisfy itself that the security arrangements proposed are compliant with data protection requirements (including the UK General Data Protection Regulation and the Data Protection Act 2018), and that the requirements relating to international transfers of personal data are met.

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 should include:

- What commitments around availability and performance of the services are being given?
- How responsive is the support that the supplier provides if the service fails / becomes unavailable? Does this flow through to service credits to compensate for the service being unavailable?
- Where will my data be held and processed (including remote access for support purposes)?
- 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? How quickly can that backup be accessed?
- What security arrangements are in place?
- What systems do I have to run in order to be able to use the service? Are there relevant formats that data / content will be stored in and are they consistent with my other systems?
- How does pricing work? Do excess charges automatically apply if the number of intended users is exceeded?
- 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?
- Is any bespoke development work required so that I can use the service, or am I taking a standard service (possibly with some customisation)?

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.

1 ICO Guidance https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/ "If specialist service providers are processing data in line with their own professional obligations, they will always be acting as the controller"

Key contract provisions

Services provided

Service descriptions in cloud contract agreements can be vague – it is important that they are clearly specified.

Key points when agreeing to 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 are likely to be pitched at the correct level to form the actual service description. It is preferable to ensure that the service description is set out in the contract rather than simply contained in a web-link
- Check whether the service is being offered on a 'reasonable endeavours' basis only, or something more concrete, such as 'in accordance with agreed service levels'
- Check whether the supplier can change or remove 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 (in which case you should ensure you have the right to terminate without cost/ liability)
- 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
- Ensure that upgrades are backwards compatible so that you can test interfaces to other systems and regress in the event there is a compatibility issue – this is particularly relevant for private cloud and/or where you have any customisations

Change in business requirements

Be mindful of your business plan when you place the initial order for your cloud service. Think further than your immediate business requirements – does your organisation have plans to expand its business or usage of the cloud?

One advantage of cloud services is the flexibility to change the level of service provided as required. A 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 and that the business clearly understands the true-up provisions that apply. Some providers will include harsh provisions for extra cost where a customer exceeds license usage

There is an increasing trend for cloud contract template terms to include verification rights for the provider to audit a customer's usage and demand payment at a much higher price for excess usage. In such cases, any subsequent delay or failure to pay these excess charges can be subject to suspension / termination rights, making this a business-critical issue

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

Key contract provisions

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. You should also check that the licence given allows you to use the service how you need to and that it does not include any restrictions which would impact your usage / your business.

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. If you are using a reseller rather than dealing with the cloud software provider directly, ensure that if the reseller has promised to ensure that you are appropriately licensed, it has the right to offer these terms to you and has backed them off with the cloud software provider itself.

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 hosted service 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 may allow for service outages which means you may not be able to access the services and your data may not be available for certain periods of time. 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 operating 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 or not functioning properly, provided that core systems can be accessed by the majority of users. Ultimately, your availability figure should mirror the time you actually need to have access to a fully functional system (or, at a minimum, 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 other customers of the cloud provider for references.

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 if there are different support packages on offer. The initial helpdesk response may simply log the problem, with a further call back to provide substantive support, and so the definition of what constitutes a response should be linked to the substantive support. It is useful to look for resolution times, as this will allow you to be aware of when your issue should be fixed.

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. Generally this will be your responsibility to check, but 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?
- Can you terminate for persistent and/or serious failure to meet the agreed service levels – this will be better than having to rely on "material breach" which can be hard to define in practice

Business continuity and disaster recovery

Given that using cloud services involves operating software and services or accessing your data from a third-party's systems, 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 ideally 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 should 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

When using a cloud application or service, you will give the supplier control over a number of areas that could impact the security of your data.

The provider

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. Companies that provide cloud computing services should look to ensure their own working practices follow best practice and demonstrate this through certification achievements such as ISO 27001/ISO 27017, Cyber Essentials, Cyber Essentials+ or NIST CSF.

Where and how your data is stored is also important. If you are investing in a cloud-based software solution, it is likely the provider will have a hosting provider partner or host their solution on one of the major platforms such as Azure or Amazon Web Services. Questions such as how they ensure the hosting service is secure are extremely important. In all likelihood, standard configuration set-ups will be insufficient and these often need additional configuration applied.

There are various industry standards that can be used to check the quality and facilities of any data centre used, including issues such as staff vetting. Furthermore, your cloud provider should undertake to audit its data centre facilities at least annually.

You should expect the provider to supply proof of penetration testing results and that these are relatively current. Annual penetration testing should be the expected minimum. This will provide valuable reassurance that both the environment and the software itself is being kept up to date with patching and the latest security best practices when developing the product. Consideration should be given to the providers own BC/DR plan, both in the sense of how they operate as a business (if they are unable to operate how will they provide you with their services?) and regarding the software solution they may be providing you with. How can they recover from an incident, what is the Recovery Time Objective (the expected amount of time a service can be back up and running by)?

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?

Other factors to consider are restrictions on access to your cloud service. Is access restricted to corporate devices provided by your business or restricted to only your own network environment? What level of encryption is applied when signing into the solution from your device to the hosted environment?

Expectations on your organisation

Cloud security also depends, to a large extent, on the measures your organisation takes.

For example, your staff should use strong passwords and make sure multi-factor authentication (MFA) is switched-on. Ideally MFA should be provided through the use of an authentication app, but at least via text or email.

Set-up of the software itself should ensure the least privilege is given to each user to ensure that individuals do not have greater access than they require. Strong password policies in place - passphrases, minimum attempts and frequency of password resetting should all be considered.

Ideally access to the cloud provider's service should not be allowed for non-corporate devices. If this is required, make sure a set of policies exists covering this type of use and that adequate technical controls are in place such as Mobile Device Management. This is important, as non-corporate devices are unlikely to have the same protections in place as your corporate devices (Anti-Virus, Web and Mail filtering options) and even if they do, they may fall out with what your own firm uses.

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 remains unclear which represent a true 'gold standard' so they should be treated with care when selecting cloud providers.

Data issues

Location of data

It is a common misconception that it is not possible to identify the location of data on the cloud. This should be considered in two strands:

- Where the data is stored or hosted at rest; any reputable cloud provider will be able to give you this information
- Where data can be accessed from (including remote access). This may be more difficult, but following the Schrems II decision, providers are being forced to track this information in order to comply with data protection requirements

The UK General Data Protection Regulation includes requirements about the processing and storing of personal data in the UK and European Union, and places conditions on the transfer of personal data to third countries (i.e. those outside the UK and/or European Economic Area (EEA)). It is recommended that you consider where your cloud provider will process, store, and transfer your data, and try to keep this within the UK and/or EEA, since this will greatly simplify the process and reduce the risk of breaches of the UK GDPR. Where data is processed, stored or transferred outside the UK and/or EEA, you should ensure that your cloud provider does this in accordance with requirements under data protection laws in relation to international transfers of data (for example, under the Standard Contractual Clauses).

Also, be sure to identify where data would be transferred to or accessed from for support, backup, maintenance or disaster recovery purposes. You will require to carry out a transfer impact assessment and put in place appropriate safeguards if data will be processed in a third country that is not deemed to offer adequate safeguards

Access to data

You should ensure that your cloud provider offers a practical method of moving your data back to you 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 provider to make available/return the data in a usable format

The provider 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, law enforcers, and the UK Information Commissioner's Office (ICO). Your contract should therefore provide for the return of your data on demand, in a readable and understandable form, even if your organisation is in breach of the terms it has in place with the provider, or if your organisation 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.

You should therefore consider the provider's data retention policy and ensure that the provider is only keeping data for specific purposes (such as to provide the cloud services or to meet regulatory or legal requirements). 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 deletion requirements should also be considered (particularly in the context of the right to be forgotten for data subjects contained in data protection legislation).

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 where your data will not be backed up and will therefore be 'lost' should the cloud system fail. Also, it is important to check that 'loss of data' is not excluded from liability. You should ensure that a cloud provider will stand behind any requirements it commits to, to back-up and securely host your data.

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

Data issues (cont.)

of the data stored on your provider's system. You should also 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. Generally, cloud providers do not to give indemnities or performance warranties for third party elements of the technology stack, with certain licences being on a 'commercially off the shelf' basis with no room to negotiate.

Data protection legislation

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 as they will not have visibility of, access to, or have any control over, the personal data that you store on the cloud. The UK GDPR places obligations directly on processors and controllers of personal data.. Any person "who has suffered material or non-material damage" as a result of an infringement of the UK GDPR has the right to claim compensation from either your organisation (as the controller) or the cloud service provider (as a processor). Accordingly, cloud service providers may seek their own warranties from you that adequate procedures are in place for data held in the cloud. You may also wish to consider seeking protections from the cloud provider that your data will be held securely and separately from other customer data held in the cloud.

In terms of the cloud agreement itself, where you are a controller and the cloud provider is a processor, the agreement should include provisions which cover the points set out in Article 28 of the UK GDPR. This includes the following:

- Be sure that the provider's role as a processor is clear, and that the provider does not have the right to use any of the data as a controller for its own purposes
- Ensure that the provider only processes the data in accordance with your documented instructions (including in relation to transfers). For transfers outside of the UK/EEA, there is now a requirement to conduct a transfer risk assessment to ensure you are satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime (and put in place adequate safeguards from a technical, contractual and operational perspective to ensure this)
- Ensure that anyone who has access to the data is subject to confidentiality obligations (including the provider's staff, and those of any sub-processors)
- The provider must agree to assist you with data subject rights as set out in the UK 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. Globally there is an increase in more comprehensive legislation on data privacy with greater awareness of privacy rights by individuals, especially in light of Schrems II. This has led to a corresponding increase in complaints and demands to exercise privacy rights
- The provider must seek prior specific or general authorisation to the use of any sub-contractors it engages that will process your data (and provide you with a right to object to any proposed updates)
- The provider must assist you with auditing or inspecting its compliance with data protection laws
- The provider must have adequate security arrangements in place, adequate safeguards and a mechanism to notify you of personal data breaches, with enough detail and including in enough time to allow you to notify regulators or data subjects within the legal time limits (see below)

You should also consider the effects of data protection impact assessments, which are mandatory for any high-risk processing. You should ensure that the cloud provider undertakes to assist you with completing your assessments and, where necessary, engages in any consultations required with the ICO.

The contract 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.

Breach notification

The UK GDPR places 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. 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 becoming aware of any breach and that they are required to co-operate with you to mitigate and resolve the breach and prevent future incidents occurring.

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 data protection legislation 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. You should push to incorporate a notice period prior to suspension, with suspension to be for material breaches only (and a requirement to restate service where the breach is remedied or if it is determined there was no breach).

Irrespective of how termination is effected, you should ensure that you have a suitable run-off period at the end of the contract (i.e. continued service provision for a reasonable period subject to the payment of fees). 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 and migrate your data.

Further information

Please contact: **professionalpractice@lawscot.org.uk**

Telephone: 0131 226 8896

This guide was produced by members of the Society's Technology and Law Committee.

Sponsor

When it comes to being cloud-based, not all legal softwares are created equally. Trust a legal software that's been offering law firms true cloud-based software freedom for over 15 years. Trust Clio.

While other legal softwares offer "cloud-based" legal software that restricts you to one device and location, Clio's cloud-based solutions allow you to work securely from any location and from any device, including a desktop computer, a Mac or Windows laptop, and from an Android or iPhone mobile phone.

With flexible contracts, low monthly costs, and 24/5 customer support, Clio is the easy-to-use cloud-based legal software trusted by over 150,000 legal professionals worldwide. Clio is an Approved Supplier to the Law Society of Scotland members. Learn more at clio.com/uk

Law Society of Scotland

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

www.lawscot.org.uk