CLOUD INDUSTRY FORUM®

Cloud UK

Paper three

Contracting Cloud Services
A Guide to Best Practice

3

Provided in association with

DMH Stallard

Executive summary

Many similes and metaphors have been used to describe Cloud Services ranging from 'elastic supply' to 'a form of outsourcing'. The challenge in entering any supply contract though is to define and embody in plain words a common understanding, set of expectations and requirements between (normally) two parties committing to a supplier-customer relationship.

The irony surrounding the coming-of-age of Cloud Services in that respect is that it is not, as so many often comment, the advent of new technology that is so compelling and valuable to the market; rather, it is the agility, scalability and almost utility basis of supply that is transforming IT procurement and challenging the way IT is purchased, provisioned and maintained. Cloud, by nature, is creating a greater sense of capability and collaboration which can, if not checked, drive contractual and operational ambiguity. This is further exaggerated when purchasing indirectly through the IT channel, which is equally caught up in the shift from pure on-premise to hybrid online solutions.

In traditional markets there is often a practical path to establish relationships between parties such as; a physical point of presence for the business supplying goods or services; a track record or a personal reference/relationship to provide that essential ingredient of 'trust' between the parties; and, clarity of who is in charge and what can be delivered. In the online world, where the number of new suppliers is growing at an astonishing rate, the traditional norms are removed and we are returned to the basic fundamental principle of Caveat Emptor or "Buyer Beware", not because there is greater risk, but because the supply model is different for SaaS and IaaS and that basic principles need to be re-established for these online relationships. In particular end users are seeking comfort on the reliability, control, integration and security of hosted services as they expand their IT infrastructure from on-premise to encompass online.

As with all new markets, there are entrants who are credible, well intentioned, capable and professional, and, there are unfortunately those that are looking to make a quick profit and whose public claims won't pass the test of scrutiny. Coupled with this is the increasing prevalence of online click-through agreements, originally designed to make procurement easier. However, after a decade of on-premise software End User License Agreements and web services agreements, this experience is to some extent muted in impact as many have adopted the behaviour of ticking the 'I agree' box to move forward in the process without the necessary caution of reading the small print. Collectively, these issues present two challenges for the would-be Cloud Service buyer:

1. How do I tell the difference between capable and rogue suppliers?

2. How should I contract for services with a CSP?

Point 1 is addressed by the CSP Code of Practice (see www.cloudindustryforum.org for details of the CoP which is designed to provide a normalised view of all credible CSPs so that an end user can make an informed decision). Point 2 is the subject of this White Paper.

To be clear though the author's over-riding position is one of complete support for Cloud Services in their manifest delivery models and alliances. That, Cloud Services will continue to grow and revolutionise access to technology for many years to come. That there is no right or wrong model, it is a matter of determining best fit and appropriate governance as well as the need for establishing clarity on how to contract and transparency of vendor capabilities and commitments.

Methodology and sampling

In early 2011, Vanson Bourne conducted research on behalf of the Cloud Industry Forum to determine cloud adoption attitudes and trends among end users and the IT channel.

The research polled 450 senior IT and business decision makers in enterprises, small-to medium businesses (SMBs) and public sector organisations.

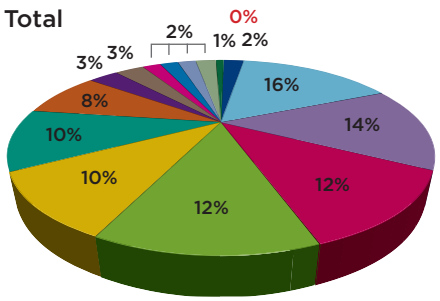
Of the 450 organisations questioned, 16 per cent came from the IT and technology sector; 12 per cent from business and professional services; 12 per cent from manufacturing and 10 per cent from both financial services and logistics. A further 28 per cent comprised of public sector organisations ranging from central to local government and healthcare.

It also polled 200 respondents from the UK IT channel, covering a broad cross section of business models and is split between IT consultancies making up 24 per cent of the sample; managed service providers at 22 per cent; systems integrators at 13 per cent; specialist resellers at 10 per cent; technical VARs at 10 per cent; IT outsourcers at 10 per cent; distributors and large resellers comprising of 7 per cent and finally IT retailers at 5 per cent.

This White Paper series summarises the results of this research and in this particular paper examines the drivers behind the legal and contractual relationships between CSPs and the end user and IT channel communities.

End user participants split by market sector:

In which sector does your organisation primarily operate?

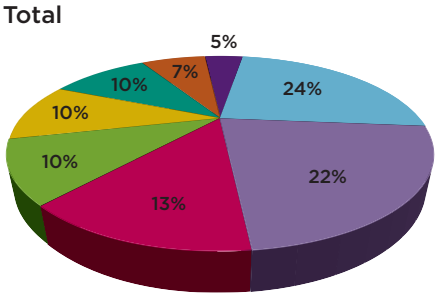


- IT and technology
- Education
- Business/professional services
- Manufacturing
- Financial services
- Retail, distribution and transport
- Local or central government
- Public sector: including armed forces and emergency services
- Public healthcare and services
- Private healthcare and services
- Construction and property
- Utilities and telecommunications
- Charity/not for profit
- Entertainment, media and leisure
- Hospitality/catering
- Other

Sample: 450

Channel participants split by IT channel type:

Which of the following best describes your organisation?



- IT consultancy
- Managed service provider
- Systems integrator
- Specialist reseller
- Technical VAR
- IT outsourcer
- Distributor/volume reseller
- IT retailer

Sample: 200

1. Survey results: maturity & consistency of Cloud Service Provider (CSP) contracting

Of all the research carried out to date for CIF, the greatest ambiguity has been seen in the results relating to the clarity and certainty end users and resellers of cloud services have in relation to their supply agreements with CSPs. A surprisingly high number of respondents accountable for cloud services stated "don't know" in response to several key questions.

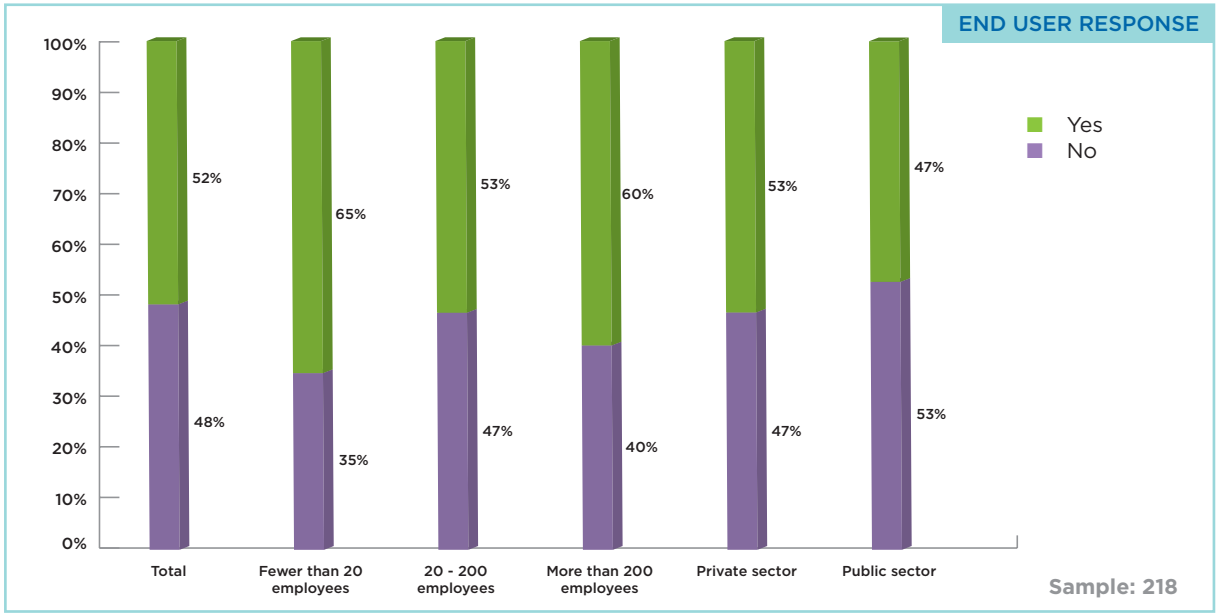
45 per cent stated they were not offered the opportunity to negotiate the contracts

The end user perspective:

As seen in White Paper 1, the most widely-represented sectors included IT and services, education, business/professional services, manufacturing, financial services, retail, distribution and transport.

With almost half (48 per cent) of organisations already consciously using cloud computing in one form or another within their organisation, it was interesting to note that only half of these (52 per cent) claim to have negotiated the legal terms of their contract with their CSP. Furthermore, the larger the organisation the far higher the chances that the terms were negotiated.

Did you negotiate the legal terms of your contract with your CSP?

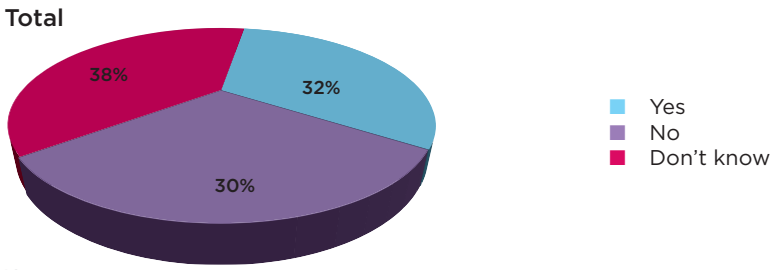


The research also highlighted that it is the private sector that is more likely to have negotiated terms with a CSP than the public. Arguably it is not surprising that the larger the organisation, the greater the chances of professional procurement officers undertaking a more detailed look at the terms and conditions of the service being provided.

45 per cent stated they were not offered the opportunity to negotiate the contracts, reflecting the somewhat customary click-thru process of software contracts that has also pervaded the online service culture. A third of the end user sample also reported that their providers could make changes to their contract simply by posting a new version online.

END USER RESPONSE

Can your CSP simply impose changes by posting a new version online?



Sample: 218

The channel perspective:

Bearing in mind that the UK IT Channel account for a significant proportion of IT sales in the UK channel research found that while only four in ten cloud resellers negotiated the legal terms of their contract with a CSP, 34 per cent did not and a further 26 per cent did not know.

When asked about their contractual relationship between their customers and the CSP some 43 per cent of resellers sign customers under their own contract, a small minority – 12 per cent – require their customers to sign a direct contract with the CSP, while some 28 per cent offer a mix dependent on which solution is being offered. In the same sample 48 per cent offer back-to-back terms between their supplier and their end user customer.

As with the end user community, the UK channel is also reporting that changes to their contracts with CSPs can be made in some 50 per cent of cases. A further third (36 per cent) do not know. But unlike the findings amongst end users, only 19 per cent of resellers claim that changes to contract terms are being imposed by posting a new version online.

UK channel is also reporting that changes to their contracts with CSPs can be made in some 50 per cent of cases

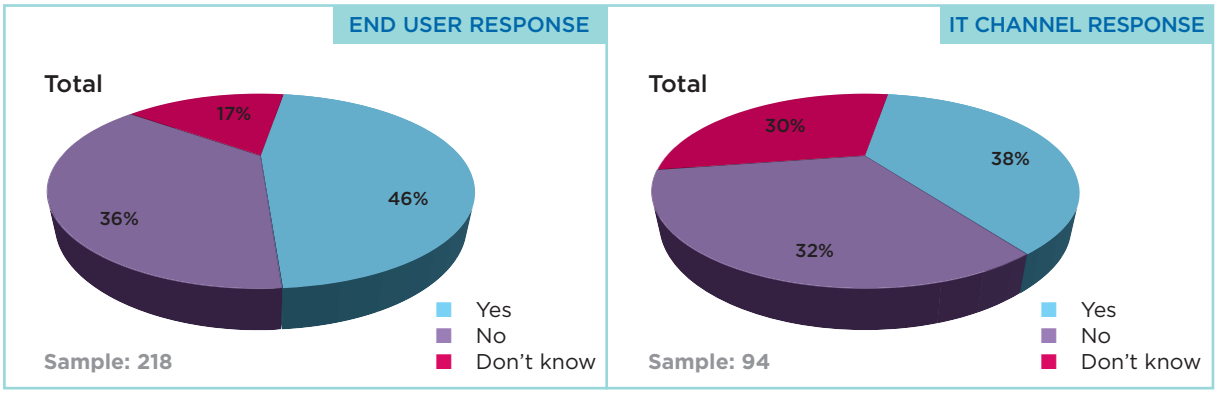
2. Key themes from the research:

Whilst the research highlighted that there was a high degree of uncertainty among both end users and resellers as to the nature of the agreements they had entered and specific terms and conditions, the following key themes were investigated:

i. **Contract automatic renewals:** Just under half – 46 per cent – of end user contracts are renewed automatically. This becomes a greater percentage the smaller the organisation. Automatic contract renewals with CSPs are far less likely to happen amongst large-scale organisations and within the public sector. Again it could be assumed that this is down to professional procurement practices associated with larger organisations, both public and private.

The IT channel also appears to reflect this with some 38 per cent of those organisations reselling cloud based services automatically renewing contracts with providers. However, and in a critical difference to the end user community, almost two-thirds of the sample has an early warning system in place as a matter of business practice to ensure they proactively manage renewals.

Is your cloud supply contract set to renew automatically?



ii. **Additional contractual protection:** End users are today looking for far greater assurances in their contracts with CSPs than the traditional service level agreement. This is more often about data and its location, security and ultimate ownership. When contracting for a Cloud Service almost 8 in ten cloud users are looking beyond an SLA for comfort in the service to be provided.

The channel are also looking for further protection and assurances. Two thirds of the channel sample stated that they wanted further assurances. These include assurances on data access and privacy controls (72 per cent), documented policies on data protection (61 per cent), accredited information management security (46 per cent) and the application of the laws of the country where the data resides 44 per cent.

What restrictions, if any, does your CSP offer in terms of which of their employees can access the data you store with them?

Only asked of respondents whose company uses cloud based services	END USER Total
There is an agreed dedicated team/group of selected employees	53%
Don't know	42%
Other	6%
Base	**216**

Only asked of respondents who resell services	CHANNEL Total
Secure authenticated connections	50%
Only those on pre-defined list	41%
Role and/or location based access	32%
Access only allowed with individually granted permission	29%
Other	9%
Base	**94**

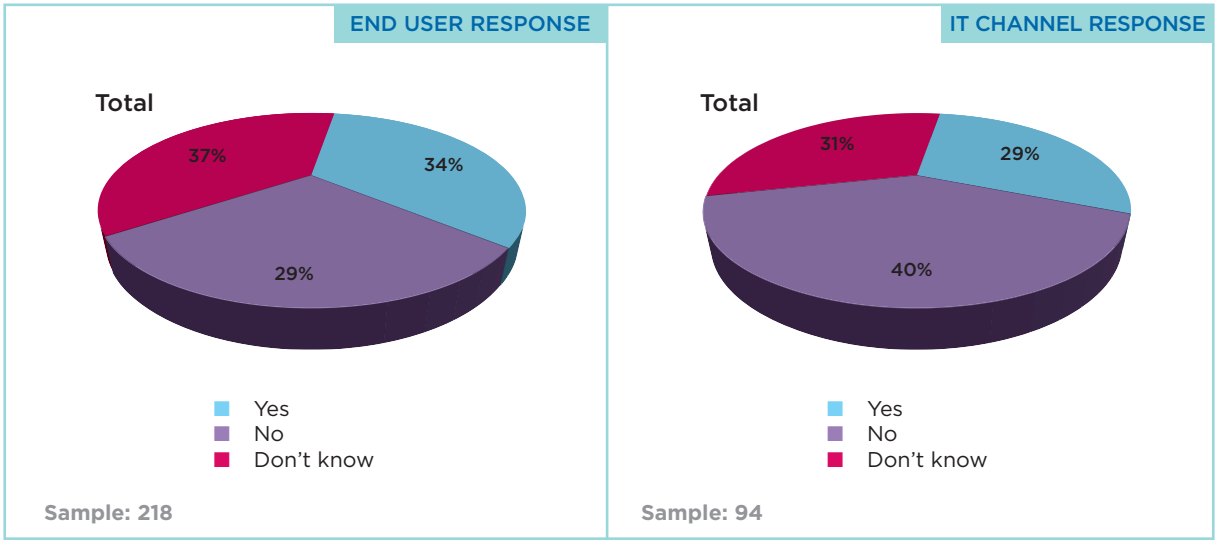
iii. **Liability for data loss:** The issue of data loss is, as highlighted, paramount in the mindset of both end users and the channel. Four out of ten cloud users reported that there is a shared level of responsibility in regard to data with their CSP. Again one key fact that stands out from closer examination is that the larger the organisation the more likely that we see shared responsibility.

According to the research just over one third of the sample – 34 per cent – report that their CSP excludes liability for data loss in their contracts. In terms of compensation that end users can claim for breach of contract and data loss, over half the sample – 54 per cent – stated that their contracts set limits.

34 per cent – report that their CSP excludes liability for data loss in their contracts

The picture is more complex amongst resellers offering cloud based services to the end user community. 40 per cent of resellers have CSP's who they claim accept liability for data loss, whereas 29 per cent explicitly do not accept liability.

Does your CSP exclude liability for loss of data?



iv. Data location: The issue of data sovereignty is critical in the mindset of many end user organisations. Amongst all users 41 per cent of the sample felt that it was vital that their corporate data was held within the UK, a figure that leapt to 63 per cent amongst SMBs and 55 per cent of public sector organisations.

Overall, 75 per cent thought it was important that their data was stored by their CSP within the UK, European Union or the European Economic Area. This figure increased to 80 per cent within the SMB sector and 82 per cent in the public sector. This has had a dramatic impact on the thinking of businesses in relation to the location of stored and processed data as the potential impact of a particular countries' laws on data storage had meant that over 80 per cent of cloud users are now more likely to demand that their data be stored within either the UK, EU or EEA.

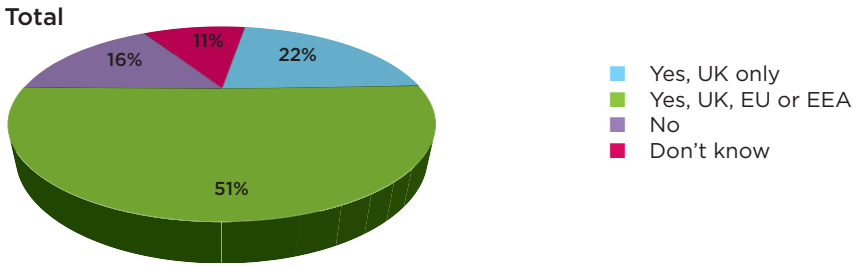
Is it important to your business that your data is stored inside the UK, EU or EEA?

Only asked of respondents whose company uses cloud based services	Total	No. employees Fewer than 20	20 - 200	More than 200	Private	Public
Yes UK only	**41%**	63%	40%	31%	37%	55%
Yes UK, EU or EEA	**34%**	17%	33%	44%	36%	27%
No	**14%**	15%	12%	15%	15%	10%
Don't know	**11%**	6%	15%	10%	12%	8%
Base	**218**	48	81	89	167	51

When the channel was asked the same questions, a slightly different picture emerged. Of those questioned 44 per cent of cloud resellers are in fact offering their services outside the EU and EEA, which gives us a more complex response. Only 22 per cent of cloud resellers felt it was important that data held remained within the jurisdiction of the UK, a figure that rose to 73 per cent when asked if it needed to stay within the UK, EU or EEA.

IT CHANNEL RESPONSE

The transfer of data outside the European Economy Area (the EU plus Norway, Iceland and Liechtenstein) is regulated. Is it important to your business whether your CSP stores your data inside the UK, EU or EEA?



Sample: 94

57 per cent had considered the legal framework of nations outside this geography and unlike the results from the research conducted amongst end users, 69 per cent of these stated that this had a direct impact on where they would insist on data being stored.

v. Data ownership: Almost three quarters of cloud users are content that their contracts within their CSPs do not allow their provider to take ownership of their – or their customers' – data or intellectual property rights.

When asked 54 per cent of the same sample believed that their provider would only hand over their data to a third party if forced to by a court order, a figure that does not alter dramatically dependent on the size of the company, nor indeed if it is public or private sector. In this case 93 per cent of end users would expect that their CSP would contact them in advance and advise them before releasing associated documents.

The research findings within the reseller community reflect a similar picture. Almost two thirds – or 68 per cent – of cloud resellers are satisfied that their contracts do not allow their CSP to take ownership of their or their customers' data or intellectual property.

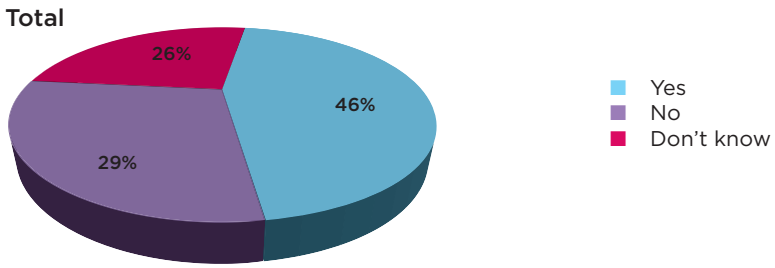
vi. **Service resilience & termination:** Of those that are using a CSP, under half (45 per cent) have a plan to migrate to another provider if the service is interrupted or terminated. Some 43 per cent do not and 12 per cent do not know.

If your CSP terminates abruptly for your breach, do you have a plan to migrate the service to another CSP?

Only asked of respondents whose company uses cloud based services	Total	No. employees Fewer than 20	20 - 200	More than 200	Private	Public
Yes	**45%**	40%	42%	51%	51%	25%
No	**43%**	48%	49%	34%	39%	55%
Don't know	**12%**	13%	9%	16%	10%	20%
Base	**218**	48	81	89	167	51

The channel research has thrown up a similar profile. Less than half (45 per cent) of resellers have a plan to migrate the service to another provider, if their existing service is terminated abruptly. And again the research indicates that less than half (46 per cent) have actively engaged with their cloud provider to define and determine what would lead to such action.

If the CSP is entitled to suspend the service in an emergency, have you defined what an "emergency" is?



Sample: 94

vii. **Insurance:** 43 per cent of end user organisations have specific insurance in the event that there is any interruption to their business if a disaster affects their providers' data centre or if their CSP leaks their data.

Interestingly 37 per cent of the sample did not know how they stood and whether they were in fact covered for this eventuality.

The overwhelming majority of end users do though, expect their provider to cover this risk. A total of 65 per cent believed this to be the case, as opposed to only 17 per cent of the sample who did not.

viii. **Acceptable use and customer status:** The overwhelming majority (70 per cent) of end user organisations have checked the Acceptable Use Policy to ensure that their CSP is comfortable with them as a customer.

Less than half of cloud users allow their CSPs to publicise that they are in fact a customer. In fact 51 per cent stated that they would not allow their CSP to publicise the fact that they are a customer.

3. The CIF Best Practice Guide for CSP contracts:

Whilst the research has shown a patchy understanding of cloud service contracts we wish to offer some general opinion on good practice. The following guidance to clarify and shape CSP Contracts is put forward to educate and inform all parties in the supply chain from service provider to channel partner to end user. The aim is to identify the common areas of ambiguity and to offer opinion on how best to approach each issue. It should be stated that by nature of commercial agreements, there is no one-size fits all approach that can be taken unilaterally and service, geography and scope will all play a part on the shape of any final agreement. However, this advice is offered to shed light on the issues that often cause the most concern for end users with a view to qualifying the underlying concerns and offering a practical approach to resolution.

NOTE: PAID FOR VS FREE SERVICE

The rights and protections that an end user will receive from a CSP will be limited where the service is offered free of charge. It is likely that a customer will recognise that a CSP will offer low (or no) levels of protection for a free service and that to get protection the customer will have to pay. For example, a webmail account or online document store will offer the customer little protection if the customer does not pay for it and that customer will have little bargaining power over the CSP to demand a higher level of protection. This White Paper focuses on paid-for services. This document is not intended to be a definitive and complete account and readers are advised they should always take independent advice when entering a new service contract.

A. CHOICE OF LAW

Overview: Contracts will often state a choice of law under which the contract will be based and reviewed and will specify which courts will have jurisdiction. A CSP will normally choose the law and courts of the jurisdiction in which its head office is based. The choice of law is generally not a contentious issue or a deal-breaker and it is legitimate for a CSP to specify that it will contract on the basis of the laws in its home territory particularly where it is offering standardised mass market cloud services. Nevertheless, customers should be aware that different laws offer different levels of protection. For example, US law – which is obviously where a number of CSPs are based – allows a CSP greater scope to limit or exclude liability. Conversely, UK legislation such as the Unfair Contracts Terms Act can allow a court to moderate or remove provisions which, for example, are unreasonable towards the user. See further analysis of this under D. LIABILITIES & INDEMNITIES.

Furthermore, even if the agreement is silent on where the CSP has its data centres or where it stores data, a choice of law outside the EU is often a good indication that the CSP will transfer data outside the EU. See further analysis of this under B. DATA CONTROL.

Customers who are looking to obtain some form of bespoke service from a CSP should raise choice of law as part of their negotiations with the CSP

Best Practice: Customers who are looking for a standardised or cheap cloud service should generally expect to contract on the CSPs standard terms including the choice of law.

Customers who are looking to obtain some form of bespoke service from a CSP should raise choice of law as part of their negotiations with the CSP. The CSP might be willing to switch this to the customer's territory or concede on other issues instead.

CSPs who are expecting to win substantial business in a particular territory should consider having a choice of law local to the customer. Clearly if the CSP has a local branch or subsidiary or if it has local data centres it can seek to localise risk, responsibility and liability to the local territory and choosing the local law is part of that.

B. DATA CONTROL

Overview: Not surprisingly, customers cite protection of data as a key issue for them. A business which currently has an on-site IT solution with its data stored in the same building or on its own private network often has the unrealistic perception that data and systems on-site are impervious to attacks or outages. Data Privacy (restriction on use), Data Security (protection from mis-use) and Data Sovereignty (storage and processing of data in a limited jurisdiction) are the three key concerns that most customers wish to see addressed.

The CSP should clearly disclose the location of its data centre/s relating to the service being contracted

No IT solution, whether on-premise or CSP based can realistically be certain to be 100 per cent immune to outages and data leaks as the risks are not fixed at a point in time. High profile outages and data leaks occur both on-premise and online, but the undue focus on cloud as a higher risk in some quarters has not helped to comfort potential customers considering a move to a Cloud Service. Nevertheless, it should be stated that a cloud solution can be structured to reliably address risks to a same or better level than the average business can achieve on-premise through appropriate process, tools and resources.

As part of a customer's need to protect its data, this often includes a desire to prevent the transfer of the data outside their territory. There is a good basis for this as the European Data Protection Directive contains a general prohibition on the transfer of data outside the European Economic Area ("EEA") (which is the EU plus Iceland, Norway and Liechtenstein) unless the destination country or territory ensures an adequate level of protection regarding the personal data to be transferred. The EU Commission maintains a list of jurisdictions that it recognises as having adequate protection. The US is not on that list but it has introduced the Safe Harbour code to protect data but this is voluntary and relies upon businesses signing up to it and adhering to the relevant levels of protection. Alternatively, a transfer of data outside the EEA is permitted pursuant to a data transfer agreement based on the European Commission's standard contractual clauses.

It is important for the customer to remember that it remains responsible for the data under the legislation particularly as, for example, the UK's Information Commissioner and the more powerful Financial Services Authority have fined organisations millions of pounds for data leaks (although CSPs have yet to be fined). Therefore, a customer must consider whether it is important that the CSP stores the data inside the EEA or whether it is content for it to be transferred outside the EEA. Storage outside the EEA is often based on location of the CSPs data centre/s, international performance (for multi regional vendors), costs of delivery and back-up strategies.

The location of a data centre is usually not dictated by data protection laws, at least, not in the first instance.

Cloud services in their current form are relatively new and CSPs do not yet have a long track record of delivery to assuage natural customer concerns. Nevertheless, it should be possible for a CSP to demonstrate that it provides an adequate level of protection for the user's data.

Best Practice: The CSP should clearly disclose the location of its data centre/s relating to the service being contracted (including back-up capability) and specify whether it offers an EEA-only base or, if it transfers data outside the EEA, what safeguards it has put in place.

Again, if a CSP is expecting to win substantial business in a particular territory, it should consider having a local data centre or partner able to meet that need.

Where the CSP has put in place a data transfer agreement, it should specify this and disclose it to customers (under confidentially restrictions if appropriate).

The CSP should also be able to specify to the customer its protocol and Service Level Agreement for restoring data from backups.

C. SERVICE AVAILABILITY & RESILIENCE

Overview: Not surprisingly, a key concern for users when contemplating cloud services is whether their data will be secure and available on-demand. CSPs recognise this and it is one of the areas that they focus on. A CSP will specify its promise of availability and resilience in its SLA together with a statement of the service credits it will offer (if any) for not meeting the promised levels. Clearly, if a customer is moving its business critical systems to the cloud, it should check the SLA to ensure it is receiving the required level of resilience. Typically all CSPs will exclude from their SLA calculations service failures due to planned maintenance, factors beyond the CSPs control (including denial of service attacks or loss of the internet) and factors caused by the customer (including misuse or incorrect use). A CSP will often exclude interruptions to service which do not exceed a specified short period.

CSPs should have documented management systems, processes and resources in order to deliver services consistently for their customers as is required for Self Certification under the CSP Code of Practice

The customer has some form of control over this by searching for a CSP that offers the customer the best service level for its needs including ensuring that planned maintenance is scheduled for times convenient to the customer (such as outside core business hours). The real test of the SLA from the customer's perspective is not just relying upon the CSP wanting to avoid damage to its reputation caused by a high profile outage, but the customer should also check what the terms specify as being the consequences where the customer does not receive this level of resilience. For example, the customer should check if the CSP offers a warranty in its terms as it is not unusual for CSPs to exclude warranties from the terms.

A further question a customer should consider is if it has not taken full advantage of any higher level of resilience offered by the CSP (probably at an extra cost) will this affect the service level and warranties offered by the CSP. Customers should note that often SLAs are defined in this manner too.

One of the difficulties that customers and CSPs face at the moment is that customers do not always read SLAs properly and CSPs do not always publish SLAs that are easy to follow. Perhaps one behaviour reinforces the other. A promise of 99.9 per cent availability does not tell the whole story by the time all the deductions are taken into account.

Finally, customers need to seriously consider the SLA they require for their business as there is a tendency to seek a 100 per cent availability even if that was never achieved on premise. As such the customer would need to consider the cost implications of such a service level, or, understand the consequence if it were not achieved. Many companies may be financially more prudent to get a better 99.9 per cent or 99.99 per cent SLA at a much more more affordable cost.

Best Practice: CSPs should have documented management systems, processes and resources in order to deliver services consistently for their customers as is required for Self Certification under the CSP Code of Practice. CSPs should specify whether the customer may audit the CSPs business continuity or disaster recovery processes .

CSPs should publish clear SLAs showing average availability times that enable their customers to identify how to obtain the level of service and resilience that they need for their business solution and be clear as to what the consequences of missing the published SLA is, whether service credits will be issued, and if so, whether they are proactively issued or have to be claimed.

Customers should evaluate the levels of availability that a CSP offers and take into account the customer's availability requirements for its business, and the price it is willing to pay.

D. LIABILITIES AND INDEMNITIES

Overview: It is commonplace for all IT providers to limit their liability and CSPs are no exception. The choice of law will have an impact (see A. CHOICE OF LAW). For example, US law allows CSPs greater freedom to restrict liability than laws in EU jurisdictions.

A CSP will tie its performance of the service to its SLA (see C. SERVICE AVAILABILITY & RESILIENCE) and customers should shop around for the one that best fits its needs. CSPs will then seek to exclude any warranties (and corresponding liabilities) implied by law or conduct – such as whether the cloud service is fit for the customer's purpose or is of satisfactory quality. Further a CSP will exclude any warranty or representation that the customer has relied upon the skill of the CSP in selecting a particular service for the customer. These exclusions are common where the customer is a business and are usually acceptable and enforceable.

A CSP in the UK will not exclude liability for death or personal injury caused by its negligence and will often accept unlimited liability (maybe even an indemnity) for breach of confidentiality or failure to comply with its data protection obligations, and infringement by the cloud service of third party intellectual property rights.

Other losses often fall into two categories: direct and indirect. Direct losses are those which arise directly from the breach and often include a customer's inability to operate due to failure of the service to operate properly. US CSPs typically seek to exclude direct liabilities as far as possible whereas European CSPs are more likely to accept some form of direct liability but exclude events outside its control, including not just so-called "Acts of God" but also such circumstances as power surges or losses. Some CSPs may seek to exclude liability for corruption of the customer's data which is stored at the CSP's data centre. Many CSPs will generally seek to exclude losses arising indirectly. These are losses that arise as a secondary consequence of the breach. Although these losses are generally considered to be more remote and less foreseeable, typically a CSP will also exclude liability for a customer's loss of profits which arise from a failure of the service and yet this is a key concern of customers.

In addition to the various liability exclusions often a CSP will seek to cap the rest of its liability to service credits or a specified amount. Typically, this amount will be a multiple of the fee that the customer pays for the service over a period of time – often 100 per cent over the last 12 months. This may not cover the customer's actual losses, particularly where a customer is moving a business critical function to the cloud.

Finally, a CSP is likely to include an indemnity from the customer to cover claims arising from the customer's use of the service, typically for infringements of intellectual property rights by the customer's content. Such an indemnity is common for social networking sites where the customer does not have immediate direct control over the users who post content.

Best Practice: A CSP should specify in clear, unambiguous language what losses it will cover and whether it will increase the cover it offers if the customer agrees to pay more or agrees to a different package of services.

CSPs should offer a service which at least complies with an implied term that is of "satisfactory quality" and "fit for the purpose" described in the CSP's published specification.

Customers should evaluate practical issues to avoid liability becoming an issue in the first place, such as resilience, failover and disaster recovery options available from the CSP.

Customers should shop around and try out the services on offer. The more valuable the customer's business is to the CSP, the more likely the customer will get appropriate protections.

A customer buying a standardised cloud service will have little opportunity to negotiate changes to the liability clause to increase its protection. But it may be able to increase its protection by paying for a Gold or Platinum service to improve the SLA. Where the customer is moving business critical functions to the cloud or is buying a bespoke Cloud Service, it should evaluate the CSP's liability cover and negotiate this to more appropriately fit the customer's requirements.

Customers should seek to specify the purpose of contracting with the CSP so that it is clear that, unless the service adequately addresses this purpose, it is pointless entering into the contract. This purpose could be addressed in the SLA. A CSP may offer an introductory period to enable the customer to evaluate the service before a full term contract comes into effect.

A CSP should consider offering a higher liability cap in return for a higher fee from the customer.

E. TERMINATION BY CSP

Overview: A customer contemplating moving to the cloud should be aware that, even though it is paying for a service the CSP will usually reserve the right to terminate its relationship with the customer. This right to terminate can be with or without notice and with or without giving a reason.

If CSPs wish to have the right and ability to terminate with a reason caused by the customer, it should honour minimum periods and should give the customer enough notice to retrieve its data and migrate the service to a new CSP

Reasons for a CSP to terminate include a variety of situations caused by the customer. The most obvious reason is where the customer breaches the agreement with the CSP. This includes breaches of the "terms of use" or the CSPs Acceptable Use Policy ("AUP"). The AUP will vary between CSPs but in essence they cover much the same ground, such as non-ownership of content, use for illegal purposes, breach of intellectual property rights, or where the customer sends bulk unsolicited commercial emails (spam). Where cloud service is for the customer's private corporate network, the customer can control this to a large extent through its own corporate policies for IT use – the customer will not want its staff to use the corporate systems for these purposes any more than the CSP will. Where the Cloud Service is for social networking purposes with general users of the service having the posting content, the customer generally has less control (although will still have policies).

Another common reason for a CSP to terminate is for non-payment by the customer. Clearly this is within the customer's control. However, termination of an account for failure to make one period payment may be unreasonable, but a CSP will terminate where the customer becomes insolvent or bankrupt or any act in the build up to this, including (if the CSP becomes aware) where the customer starts negotiations with creditors, a company begins winding up procedures, or an administrator or administrative receiver is appointed over the customer.

A CSP may also terminate where the customer's account becomes dormant through non-use or the death of the contracted party.

So, CSPs have the right to terminate for a number of reasons and customers should be aware of these. While a customer will often have the ability to prevent termination by the CSP for a given reason – by ensuring that reason does not arise – the customer should be aware of the CSP's ability to terminate without a reason (caused by the customer) as the customer is likely to have invested a great deal of time and money setting up the service and ensuring it is compliant with all of the CSP's terms.

In reality, a CSP may still have a reason to terminate a relationship with an otherwise compliant, paying customer. This might be following a re-evaluation of the CSPs portfolio, a restructuring of the service portfolio following acquisition or sale of its business or perhaps because the CSP has gone out of business. In most scenarios, a CSP will usually give a customer notice that it is about to terminate. The customer should check this notice period and decide whether this will be enough time to transfer the service to an alternative CSP.

Except for customers which are in breach, a CSP will normally grant customers the chance to access the customer's data during a grace period after the CSP has given notice of termination, during which time the customer can transfer the data to another CSP.

Best Practice: It is legitimate for the CSP to terminate for a reason caused by the customer, including breach of terms of use or the AUP, non-payment, insolvency of the customer. A customer will be faced with similar terms from most CSPs and should not expect to be able to break the law or violate the AUP without consequence.

If CSPs wish to have the right and ability to terminate with a reason caused by the customer, it should honour minimum periods and should give the customer enough notice to retrieve its data and migrate the service to a new CSP.

The CSPs agreement should not entitle it to change the terms without the customer's consent or, at worst, the CSP should give customers notice of those changes allowing the customer to decide whether to terminate if it disagrees with the changes.

The CSP should preserve the customer's data following termination. See F. DELETION OF DATA.

F. DELETION OF DATA

Overview: The CSP will include in its agreement the right to delete a customer's data in a number of scenarios.

CSP agreements should contain a general rule that the customer is to control when data is deleted

A CSP will normally seek to delete data where there is an issue regarding the customer's content, for example, it believes the customer is in breach of the CSP's terms of use or AUP. As a CSP can be liable for failing to take down content which is offensive, defamatory or that infringes intellectual property rights, it will usually reserve the right to delete such data. What is offensive, defamatory or constitutes an intellectual property rights infringement is often subjective and the CSP is more likely to want to protect itself against liability than to protect its customer's data. In such a situation, the CSP might not give much or any notice of the suspension or deletion and, in any event, is likely to terminate its relationship with the customer (see E. TERMINATION BY CSP).

Where a CSP terminates for reasons other than those connected to legality of content it may give notice or allow a grace period before deleting the customer's data. Customers may face additional charges to access their data during a grace period.

Some CSPs may automatically delete data at termination (without any notice). If the CSP's termination is wrongful, and the customer's data has been deleted, the customer will have to consider whether it can obtain any compensation from the CSP and whether this is likely to adequately cover its losses (see D. LIABILITIES & INDEMNITIES).

Of course, a CSP will generally delete data at the customer's request (provided the CSP does not retain a copy in case there is a court case). The customer generally has control over this deletion save where customer has granted a licence to the CSP to use the customer's data for its own purpose. This licence may survive after termination, meaning that the customer's data is never truly deleted. However, this is more likely in a social networking example or where the user doesn't pay for the service.

A CSP might delete data by accident or where the data becomes corrupt. Data recovery is vital to a customer and is often the specific purpose for which the customer has signed up. Data integrity is likely to be improved if a customer pays for the CSP's backup or failover service. The service level agreement should define the CSP's data retention obligations and the customer should review this carefully.

Best Practice: CSP agreements should contain a general rule that the customer is to control when data is deleted.

In all circumstances, including termination, the CSP should preserve the data even if it does not make it directly available to the customer. Where a CSP wishes to delete unlawful data, the CSP should quarantine the data and suspend the account. This will allow courts to resolve disputes – for example to allow a court to rule whether the content is actually unlawful– or will give the customer a chance to pay sums it owes.

Where a CSP wishes to delete data upon termination, the CSP should notify the customer specifying a time period of at least 30 days. The CSP should also assist the customer with migration or at least allow sufficient time for the customer to migrate data by itself.

G. SERVICE TRANSFER

Overview: The general rule is that customers are free to choose their CSP. As the cloud and the number of CSPs grows, customers have more choice and are more willing to transfer between CSPs. However, this freedom to transfer is likely to be limited by commercial, technical and practical CSP lock-ins.

The CSP should offer a data migration service with a clear charging structure, if a charge is appropriate

A CSP can effectively lock in a customer through commercial terms: that is, long periods without break clauses and with penalties at the end of service (including monetary penalties and/or exclusions or limitations on the customer's access to its data). The customer can, to a degree, control this by reviewing these clauses and negotiating suitable provisions or signing up with another CSP.

A CSP can also lock in a customer through technical measures such as where the Cloud Service uses a proprietary system. While the onus will usually be placed on the customer to retrieve data to enable a transfer to a new CSP, the data may not be in a transferable format that is in an industry standard or open format. There may be no contractual obligation on the CSP to convert the data so that it can be transferred but the CSP might be willing to do this for an additional fee. The portability of data is a matter for the customer to assess prior to signing up with the CSP.

Finally, a CSP might lock in a customer through practical issues – that is, the amount of time, effort and money that it will take a customer to migrate the service decreases the incentive on the customer to move. Costs may include end-of contract penalties imposed by the CSP (particularly if the customer seeks to terminate part way through an agreed minimum term), format conversion of the data and transfer fees. If the customer has a lot of data stored with the CSP in non-standard format, the effort to convert this and the CSP's fees for doing so might mean that the customer does not move services. Again, this is a matter for the customer to assess this prior to signing up with the CSP.

Best Practice: The CSP should offer a data migration service with a clear charging structure, if a charge is appropriate.

The CSP should specify (if it is not already obvious) whether its systems are proprietary and not interoperable with recognised industry standards.

Where a customer wishes a CSP to transfer service and data outside the EEA (where it is currently inside EEA), the CSP may look to the customer for an indemnity for breach of data protection legislation (provided the CSP itself complies with relevant obligations under legislation and instructions of the customer).

Also, a CSP should provide reasonable assistance to migrate service to a replacement CSP and have a clear policy so the customer knows what help it will receive and how much this will cost.

4. Conclusions

The research carried out for the Cloud Industry Forum has highlighted a fragmented approach to contracting with CSPs, where consistency, clarity and transparency appear to be lacking in either or both the agreement or the procurement process.

We can conclude:

1. Whilst the private sector end user is arguably leading the charge on contract negotiations and changes, contracts between cloud resellers, CSPs and end users are generally fluid and service dependent.

2. There is not, and the market does not require, a one-size-fits-all agreement (as by nature the notions of shared vs private services and SaaS vs IaaS have fundamentally different requirements, responsibilities and structures). However, there is a need for clarity and transparency in all contracts on key issues that impact and concern end user organisations as set out in the Code of Practice.

3. Data Security, Privacy and Sovereignty are key issues to be covered off in any agreement including clarity on CSP liabilities for direct and indirect loss.

4. Local law, local data storage and proven record are more important to the majority of end users than most other issues. Flexibility by CSPs to provide proactive comfort on these topics in their agreements will be received well by end users.

5. A number of cloud services involve multiple parties in the supply chain. Contracts should make clear where necessary if there is any data sharing with third parties to achieve the service and identify what protections are in place or liabilities exist for the end user if they are not covered by the CSP automatically.

6. There is an absence of formal Standards in contracts and without restricting commercial advantage the industry would benefit from adopting best practices which can be shared and embodied in CSP contracts, to provide clarity on key issues of concern for end users.

7. The end user should always assume and maintain ultimate responsibility for decisions they make either on-premise or in terms of adopting Cloud Services, and good governance requires them to be clear on their choice, their backup plan and their insurance cover. Whilst a CSP can be held accountable for a breach of contract or a service failure, the end user still needs to be clear on what their remediation plan is. The absence of one is a critical flaw in any sourcing decision. There was not clear evidence in the research that appropriate due diligence was taking place.

8. CSPs have an opportunity to achieve competitive advantage by being both easy to do business with and by being straightforward to do business with. Clarity of obligations, service levels, service options and issue resolution will positively reduce risk for end users in making their supplier choice decisions.

9. There is a proven benefit for CSPs to be certified to provide an independent frame of reference to compare and contrast differing CSPs. This was endorsed by 83 per cent of end users and 72 per cent of cloud service resellers.

CLOUD INDUSTRY FORUM

7safe
Microsoft
APM Group
Accrediting Professionals
nominet
ChannelCloud
Designed by the Channel for the Channel
OUTSOURCERY
CHANGING WORK FOR GOOD
DELL
rackspace
IT HOSTING
FAST
Federation Against Software Theft
RISE
fasthosts
Scalable
FrontRange
SOLUTIONS
ScienceLogic
interxion
UKFAST
intY
Software-as-a-Service
webroot
MAMUT
www.mamut.com
Business Software
UK PLC

The Cloud Industry Forum (CIF) was established in direct response to the evolving supply models for the delivery of software and IT services. Our aim is to provide much needed clarity for end users when assessing and selecting Cloud Service Providers based upon the clear, consistent and relevant provision of key information about the organisation/s, their capabilities and operational commitments.

We achieve this through a process of self-certification of vendors to a Cloud Service Provider Code of Practice requiring executive commitment and operational actions to ensure the provision of critical information through the contracting process. This Code of Practice, and the use of the related Certification Mark on participant's websites, is intended to provide comfort and promote trust to businesses and individuals wishing to leverage the commercial, financial and agile operations capabilities that the Cloud based and hosted solutions can cover.

The Cloud Industry Forum

Sword House, Totteridge Road, High Wycombe HP13 6DG
t 0844 583 2521 **e** info@cloudindustryforum.org
www.cloudindustryforum.org

DMH Stallard is a law firm whose lawyers continue to lead thinking in the technology sector. We are proud to work with some of the most innovative and successful organisations in the country including major financial institutions, many FTSE listed companies, private equity backed businesses and high profile public sector bodies.

DMH Stallard LLP

6 New Street Square, New Fetter Lane, London EC4A 3BF
t 020 7822 1500
www.dmhstallard.com www.tomilaw.com