UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Cloud Computing: A flexible solution or an IT straightjacket?

Valerie Taylor reports on the Society for Computers & Law Seminar 'Cloud Computing – How it can be made to work', and examines the view from both extremes.

"Skeptics in the Pub" is a discussion group that has recently enjoyed an upsurge in popularity after being featured in several national newspapers. The group arranges meetings for those interested in science, history, philosophy, investigative journalism and how to examine extraordinary claims of all kinds. Cloud computing: the saviour of modern IT or just another way for the likes of Amazon, Microsoft and Google to make massive amounts of money and take control of our data? Perhaps this will be on their agenda soon.

At the Society for Computers & Law seminar on 24 March, speakers from a variety of organisations debated the pros and cons of cloud

Continued on p.3

Data protection considerations in cloud contracts

Organisations may wish to negotiate changes to the cloud providers' standard contracts. **Renzo Marchini** explores the key data protection issues to be included.

Enterprises going into a cloud deployment will have many concerns. This article examines how cloud contracts can deal with one of the more common concerns: information security and data protection.

Before we look at the contract, we set out as a quick reminder the main such issues which arise:

- Any customer (whether processing personal data or not) will first and foremost want to ensure that the data is kept secure. In the context of personal data, this is reflected in the seventh data protection principle: the obligation to take appropriate security measures.
- A customer will need to know if

Continued on p.4

Issue 55 **May 2011**

standard terms of many service providers state that it is the user's responsibility to ensure the security of their own content. How do you do that? Do you back up in another cloud or use your own servers? If you are concerned enough that you use your own servers to back up the information you have in the cloud, doesn't that defeat the object?

Sony's experience highlights the reason that the cloud is successful – the economies of scale are available because the service on offer is a standard one. If your business needs do not fit the standard model, you will need to negotiate or look elsewhere. There is a gulf between, on the one hand, the cloud companies' standard terms for a service designed as a utility for SMEs, and on the other, the expectation of larger organisations that they will be able to negotiate the terms of supply. What this may reveal is that smaller businesses will have no choice but to accept the suppliers' standard terms whereas large enterprises, such as Sony, will be able to use their muscle to negotiate bespoke security offerings and enhanced service levels.

Can there be a conclusion?

The electricity analogy is very persuasive. Why bother with all that hardware and associated stress and responsibility if you can get someone who is better equipped to do it for you?

There are a number of concerns about entrusting IT services to a third party in the wholesale manner demanded by cloud computing. It is not just the hardware and software that is at stake, it is the content of those systems – the precious data that most organisations value as their lifeblood, be it personal data about clients or confidential business data.

The cloud service providers have access to a vast amount of data. Clearly they will be bound by confidentiality agreements and no reputable provider would be in business for long if they were found to be deliberately exploiting their clients' data for other purposes. However, there have been cases where cloud service providers have lost client data. Online storage provider The LinkUp shut down a couple of years ago after losing unspecified amounts of customer data.

Finally, there is the power associated with the fact that a few big cloud providers manage so much of the world's data resources. There have been concerns for years over Microsoft's dominance in the software market, and new concerns are arising about Google's analysis of individuals' web surfing habits (invisible to many users), as well as their inadvertent capture of WiFi transmissions as part of their Street View service. If major (and minor) businesses entrust their data to these same service providers, does this not give them power beyond measure? Something for the Skeptics in the Pub to consider, perhaps.

INFORMATION

See www.scl.org and www.skeptic.org.uk/events/skeptics-in-the-pub

Protection... from p.1

personal data will be sent outside of Europe. If so, how will adequacy be assured to comply with the eighth data protection principle and how should the contract reflect the adequacy solution adopted?

There are other information security and data protection issues, of course, but these will be the main ones.

Contracting for the cloud

Providers will have their standard form of contracts. Implicit in a discussion of what a customer should look for in a cloud contract to deal with the information security and data protection issues, is the idea that the provider will entertain a request that it departs from its standard terms and negotiates. One aspect of cloud computing which is often cited as being different from other technology deals is the take-it-or-leave-it aspect of the technical solution. In keeping with the commercial and technical advantages of the solution being easy to set up, easy to scale, and easy to control charges, it is also equally easy to contract: a customer simply accepts the provider's terms without question.

This is very true in relation to many provisions available at relatively low cost and possibly without any interaction except through the provider's website ("click-wrap terms"). It is not however true of substantial acquisitions by enterprises. Contracts are still individually negotiated. Whilst many cloud providers may present their contracts as standard and not invite negotiation, nonetheless, customers can request changes to the "standard". Whether the provider agrees to those requests will depend on the negotiating power of the customer. Consumers and most small businesses, each acquiring a very standard cloud offering, will have no scope for negotiating terms. However, that is not the case for substantial enterprises negotiating as equals with a cloud provider. The bigger the potential contract, the greater the scope for the cloud provider moving from its standard position to secure the deal. The City of Los Angeles certainly negotiated its contract with Google (and CSC as implementing consultancy) in its high-profile SaaS deal.

Where contracts are not negotiated, as a recent study makes clear[1], many providers accept very little liability at all (if any) for data security breaches and problems. This article, then, describes the data protection issues which arise in the cloud and describes the types of provisions that may appear in a negotiated cloud contract to deal with them.

Preliminary issues – controller or processor?

The use by a cloud customer of a provider to process its data invokes a consideration of whether the provider is a data processor or a data controller. If the provider is a processor, the main compliance concern is for the customer to ensure it satisfies the seventh principle (to keep data secure). If the provider is a controller, the additional concern arises as to how the disclosure to the cloud provider can be "fair and lawful" as required by the first data protection principle.

Many cloud providers would hope that they would be considered to be a processor (and thus avoid various regulatory obligations). Nonetheless,

following the EU Data Protection Working Party's SWIFT decision and the Working Party's subsequent opinion on these important definitions[2], it is not possible to be absolutely certain that this will be the case in the eyes of regulators and enforcement agencies.

Given this difficulty, and the risk of regulatory or legal action if a wrong characterisation is made, a potential cloud customer intent on guaranteeing its compliance with the DP Act would do well to have regard to the possibility that the cloud provider is in fact a controller.

Cloud provider as processor

When a processor is appointed, the seventh data protection principle requires the customer to ensure the provider gives "sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out", and takes "reasonable steps to ensure compliance with those measures".

As is well known, there must be a written contract in place and that contract must oblige the processor to act only on instructions from the customer and require the provider to comply with obligations equivalent to those of the seventh principle. We return to this below, but note here that due diligence into security will be required.

Cloud provider as controller

If the provider is a data controller, then the act of the customer in putting the personal data into the hands of the provider is an act of processing which needs to be "fair and lawful" under the first data protection principle. The customer is likely to be able to rely – in most circumstances – on paragraph 6 of Schedule 2: when the processing is necessary for the purposes of "legitimate interests" pursued by the customer (e.g. the cost-effective acquisition of computing resource)[3]. The test however also contains the proviso that the processing must not be "unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject". An appropriate risk assessment in relation to the cloud service (including due diligence) is likely to be needed before the customer can assure itself that the cloud service would not unduly prejudice the rights of the data subject.

Does it matter?

As we have just discussed, due diligence will be required whether the provider is truly a processor of the customer's data or rather a controller. From a customer's perspective, a contract limiting use of the data to the provision of the service will be needed under either characterisation and it is hard therefore to see any real difference (assuming there is a legitimate basis for the processing) from a customer's perspective (at least, when non "sensitive" data is involved). From a provider's perspective, of course, a designation as a processor would matter as the provider may then be subject to the principles (if based in the European Economic Area).

Ensuring security and the seventh principle

The minimum

The contract should set out an obligation upon the provider to comply with a particular security standard. At a minimum it could be in general terms such as, "the provider will use reasonable efforts to keep data secure". Most contracts in the cloud will say no more.

It would be better, as far as the customer is concerned, to set out some level of detail about what in fact will be provided. This would often be in the form of a security schedule tailored to the particular customer's concerns and risk appetite.

Here we get a tension with the cloud model. The economics of the cloud depend on it being a standard offering, perhaps running software shared by many clients (so called multi-tenancy architecture, where the same instance of the software services the data of a number of clients at the same time). As such, the provider is not able cost-effectively to tailor its security mechanisms for specific customers. Nonetheless, if the customer is big enough commercially and the contract is valuable enough, greater assurance might be offered.

A tailored security schedule

Prior to considering signing a contract, a customer would have undertaken some level of due diligence into security standards. The extent and depth of the diligence to which the customer will go depends of course on the type of service, the value of the contract, the sensitivity of the data, and other such issues. As part of a diligence process, the provider will either, by reference to publicly available policies (perhaps on its website) or in response to questionnaires, supply the customer with some detail around its security policy.

To proceed any further, the customer will have been satisfied with the response. If anything was particularly important to the customer, the customer should ensure that that particular point is covered in the agreement. For example, if sensitive data is being put into the cloud a particular strength of encryption article might be specified.

Information security standards

Another approach being seen in relation to security is reliance on a recognised security standard. Compliance with and/or certification to certain security standards will often be cited by cloud providers; partly to avoid repeated requests to respond to security questionnaires or to permit an audit.

The ISO 27000 series of standards addresses information security management and includes (in ISO 27001) a certification process in relation to information security management systems (ISMS). Certification when achieved is a real measure of commitment by a provider. However, a customer should not rely on certification without at the very least checking that the scope of the ISMS covered by the certificate includes all aspects of the cloud solution the customer is considering acquiring.

SAS 70 is a standard often mentioned by cloud providers. To give it its full name, the Statement on Auditing Standards No. 70 is a standard developed by the American Institute of Certified Public Accountants (AICPA). It is not a security standard; it is only an auditing standard. The cloud provider is free to set whatever controls it wishes and the audit describes those controls and the objectives they are intended to achieve. Given the lack of prescription as to the controls to be included in any information security system, great care is needed by a customer in relying on the existence of even the more rigorous SAS 70 Type II report. Any report will certainly need careful scrutiny.

Once a customer is satisfied with the certification being asserted, the contract could contain an obligation to ensure the certification is maintained for its term.

Ongoing monitoring: Contractual rights to audit?

A further requirement of the seventh data protection principle is to take "reasonable steps to ensure compliance with those security measures". This is often interpreted to require the contractual ability physically to inspect the provider's facilities, but the obligation may not go that far. If that is what is required, then in a full "cloud" procurement involving data being located in multi-tenanted virtual servers in unspecified locations (perhaps simultaneously and ever-changing) or simultaneously in multiple locations, it would be nigh on impossible to acquire cloud services when personal data was involved.

Nonetheless, cloud deals are happening and customers are taking the view (if they are not ignoring the issue) that this aspect of the seventh principle might be complied with by other controls, such as a requirement for full monitoring and reporting by the provider itself or to undergo full security certification by an accredited organisation.

Location of the data and the eighth principle

Some vendors recognise the restrictions in the eighth data protection principle and are willing to give the assurance that data will remain in a particular country (perhaps for additional fees). Some of the major IaaS providers, for example, will tell their European business customers for at least some of their products that data will reside only in European server farms.

Other providers, salesforce.com, for example, openly state that their data will not remain in Europe. If this is the case, then one of the various mechanisms to legitimise that transfer under the eighth principle may well need to be put in place.

The following options are available:

- **Keeping data within Europe or in a country deemed automatically adequate**: If this is being relied on, then of course the contract should contain a binding assurance from the provider to keep data in that country.
- **Safe Harbor**: A US cloud provider could be on the Safe Harbor list (Salesforce.com and Google are), and provided the certification is up to date and relevant to the data being transferred it is a good solution for the customer. Again, a customer – as controller – should do what it can to ensure that the provider remains on Safe Harbor. The contract should contain a commitment upon the provider to maintain its certification and to comply with the scheme.
- **Standard clauses**: These are another solution which generally works well from a customer's point of view. The EU clauses will sit alongside the "commercial" contract and the latter need have (from the transfer perspective) no other provision. There is at least one difficulty, however: which clauses should be used? The controller to processor clauses are the most natural ones, but – in the light of the SWIFT decision and the subsequent Working Party opinion (discussed above) – will the provider always be a processor? Cloud providers outside of the EEA will not necessarily sign the standard contracts. After all, they do increase their potential liability above that which may have been agreed in the "commercial" contract.
- **Self assessment**: A customer could "self-assess"; that is, reach its own view that the personal data once transferred is adequately protected. In many cloud situations, when (i) the data is not particularly sensitive, (ii) a sensible security diligence has been undertaken, (iii) proper contractual language is in place dealing with security, and (iv) the cloud provider is a reputable company of substance, it will not be unreasonable for the customer to satisfy itself that there is adequate protection. With this approach, other than dealing with the seventh principle issues already discussed, the only contractual provision needed is the assurance that the data will remain in the country upon which the assessment was based.
- **Other methods**: For completeness, it is worth noting that there are other methods for legitimising transfer although they are unlikely to be helpful for most cloud solutions. Binding Corporate Rules facilitate transfers throughout groups; as such they may be of use in relation to so-called "private clouds" but not otherwise. The derogations such as consent (which needs to be specific and informed) and necessity for contract performance are unlikely to be useful.

Conclusion

As can be seen, a contract can assist in navigating the data protection compliance issues which a customer will be faced with. Whilst the characterisation of a provider as a "controller" or "processor" can under the present law be difficult, we have seen how from a customer perspective it may mean very little difference in practice. Indeed, the distinction may well not survive the ongoing review of the EU Data Protection Directive. Lastly, it goes without saying that the contract will deal with many other data issues, including provisions dealing with matters which, although not strictly required by data protection law, may be advisable; such as, an obligation for the provider to inform the customer in the event of a data breach or in the event that a law enforcement agency (whether of the UK, a US agency under the US Patriot Act or otherwise) makes an evidential request which involves the data.

REFERENCES

1. Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, 1st September 2010, Queen Mary, University of London.
2. Opinion 1/2010 on the concepts of "controller" and "processor", WP 169 of 16 February 2010.
3. However, if the cloud service is to involve "sensitive personal data" – it is hard to see which of the Schedule 3 conditions might be relevant.

AUTHOR

Renzo Marchini is Counsel at Dechert LLP and has just written a book *Cloud Computing. A Practical Introduction to the Legal Issues* (BSI, November 2010), which explores the issues of this article in greater detail.
Email: renzo.marchini@dechert.com