

write news

Clear, pragmatic and commercial legal advice on
all aspects of IT

The articles in this newsletter are for guidance only and do not constitute legal advice.
The firm is regulated by the Solicitors Regulation Authority.

- 01/02 Cloud Computing
 - 03 Working with Data Off-Site
 - 04 Software Patents Update / Cookies
-

Cloud Computing

As many of you will know, cloud computing is an up-and-coming alternative method of providing access to IT infrastructure and services to clients. Cloud computing involves the supplier or "cloud provider", offering IT facilities through the Internet or the "cloud" infrastructure. Such facilities and infrastructure normally includes the provision of remote platforms and/or user/sector specific applications, storage and/or online support services.

If you are considering providing your software, infrastructure or platforms to your clients via the cloud, you should consider our top ten legal issues concerning cloud computing before you proceed on this basis.

Top Ten Legal issues concerning the Cloud

1. Minimum requirements

The selling point of the cloud is that it offers flexible IT resources usually on a pay-as-you-use basis with clients only paying for the capacity and services they require as and when they need them. That said, you should consider whether you will require a minimum monthly payment for the provision of your cloud services from clients and/or whether any under-use or over-use will be credited or debited from future invoices on a month-by-month basis.

2. Flexible IT resources

Another main advantage with the cloud in the current economic climate is that the IT resources your clients' businesses require can be increased or decreased immediately according to their business needs, without clients having to predict their future IT requirements months in advance. However, you should consider how much notice you require if your client wishes to change its requirements and to what extent you should be contractually obliged to meet their new requirements taking into account your processing and storage capacity. You also need to ensure your agreement with your client contains adequate provisions to vary fees and/or services.

3. Liability for service failure

Theoretically the cloud should be a robust service but no IT service is ever 100% free from the possibility of there being downtime or service availability issues and the IT infrastructure in the cloud is no exception. Downtime may have a significant impact on your clients' businesses and the cloud provider could be exposed to significant losses. Therefore cloud providers should consider including a variety of exclusions of liability, in particular in relation to liability to clients disruption to business and loss of profits.

4. Service level agreements

Careful consideration needs to be given as to whether you are prepared to offer minimum service levels of up-time and whether any credits will be given if service levels are not met. Although the client may have redress against the cloud provider in such circumstances, i.e. reductions in monthly payments, it should be borne in mind that this may not be adequate or appropriate in light of a client's business requirement. Do customers need to use the service 24/7 or just in working hours? It is also worth considering whether service levels can be agreed at all, as any amount of downtime may be business critical to your clients. Typically, scheduled downtime perhaps at certain "off peak" times of day is excluded from any service level obligation.

5. Clients' liability

It is common for cloud providers to require IP and data integrity warranties and indemnities from clients on the basis that clients' data uploaded to the cloud should not breach a third party's intellectual property or data protection rights. Clients should also be under a strict obligation to keep passwords secure and take steps to avoid any unauthorised access to the cloud.

6. Data Protection

The very nature of the cloud raises questions regarding data protection and security. You should consider whether the cloud services being offered involve the transfer and storing of data outside the UK. Any such transferring, processing and storing of personal data must comply with the Data Protection Act 1998, particularly if data is to be transferred to or stored in a country outside the European Economic Area. If data is stored in a different jurisdiction, it may be subject to local laws which can in certain circumstances allow such data to be accessed for reasons of national security.

7. Control of Data

Inherent in the use of the cloud is that an element of control over data passes to the cloud provider. Clients may require detailed provisions placing strict limitations on the cloud provider regarding use of and access to such data. Ownership of all data should remain with the client. You need to consider what is to happen to the data if a client wishes to terminate your services and go to an alternative cloud provider. Data should be returned immediately but in reality there may be a delay if, for example, the new provider's systems are not compatible with yours. Who is to pay for any additional work that may be required to make such data/services compatible? What is to happen if a solution cannot be found and will you provide a run-on service in the interim?

8. Delay and Third Party Comms

The benefit of cloud computing and remote access from any computer to services or data may also be its burden as it relies on good communication links and problems with connectivity or networks can cause delays. Therefore, easy access to services and/or data is not always guaranteed due to failures outside the cloud provider's reasonable control. Such matters should be excluded from the cloud provider's responsibility so that the cloud provider does not accept liability for such delays and any resulting losses suffered by the client.

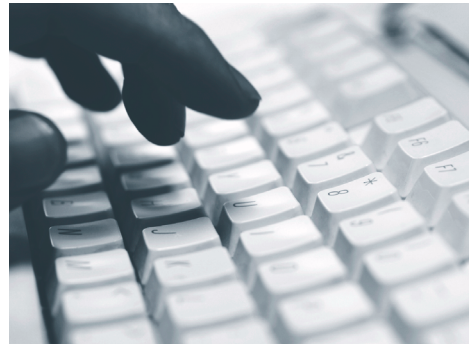
9. Licensing

If your cloud service relates to your proprietary software, the ownership of such software is important. Where the cloud provider is the owner, then the client will be granted a licence to use such software as part of the cloud service. The scope and restrictions placed in such licences are very important as they will often in themselves define the business model by which a cloud service is deployed. If the software is owned by a third party, then you must ensure you have the right to sublicense and provide the software to the client as part of the cloud services.

10. A green service

Cloud computing may enhance a business's corporate social responsibility as it is seen as environmentally friendly. Cloud computing is a modern development, as are the systems used to provide the services and therefore, through the use of the cloud, a business could reduce its carbon footprint.

Cloud computing is a relatively new concept and is likely to take some time to evolve and develop standard practices. Therefore, if you are considering providing cloud computing services, it is important to have a detailed contract in place with your clients that takes into account the practicalities and realities of providing cloud services.



Working with Data Off-Site

In recent years due to advances in technologies, IT facilities, clients' requirements and employers' obligations to consider flexible working and working from home requests, many employers either allow or need their employees to work off-site at home or at client premises. Such method of working is often as effective as working in the office as it is easy for employees to gain the same access to the same data and information as they would be able to access in the office off-site. It may be an attractive and sensible option for employers to allow employees to work off-site. However, employers should consider the following when allowing employees to work off-site and ensure that certain safeguards are in place.

1. Data Protection

One major issue associated with working off-site is the use, storage and disposal of data and confidential information. The Data Protection Act 1998 (the "DPA") imposes a variety of obligations on employers to ensure that they process personal data fairly and lawfully. Businesses are also often bound by confidentiality and data use agreements requiring them to keep client data confidential and secure. As many of you are aware, there have been many high profile cases of computers containing confidential personal information being left or lost on trains and it would seem to be only a matter of time before similar cases are reported of data being found on misplaced memory sticks. It is all too easy for employees to carry important personal and client data around with them when they are working off-site.

2. Equipment

Businesses should consider what equipment is required to be provided in order for employees to work off-site and who will provide such equipment, the employee or the employer. If the employee is to provide the equipment or use their own computers, you should consider whether such equipment is compatible with the software and/or services to be accessed by the computer in order for employees to fulfil their role. You should also consider who else has access to the computer, particularly if it is a family computer, and whether such individuals could access the employers' and/or clients' data and records. Taking this into consideration, many employers prefer to provide the equipment for employees to use, as the employer has greater control over the use of the equipment and access to its data and/or records.

3. Software Licensing

If the employee's role relies on access and use to any specific third party software you should review the terms of your software licence. Can the software be installed on the employee's home computer? Is the software licensed to particular users or permitted terminals and therefore will additional licences be required?

4. Passwords and Security

Regardless of whether employees are using their own equipment, their employer's equipment, accessing services via Cloud Computing or via servers, employers must ensure that all systems, software and servers are password protected or encrypted and that employees are under strict obligations to safeguard such passwords and take precautions to ensure there is no unauthorised access to employers' data and systems. It is essential that employers have detailed written security policies in place for information taken and accessed off-site by their employees, clearly stating how any confidential and personal information should be used and protected off-site to ensure that it does not get into the wrong hands. If a business is found to have breached the DPA and confidentiality then there could be serious consequences imposed against the employer, including substantial damages which can have a damaging effect on the business and its reputation.

It is wise for employers to consider having such policies linked to its employees' disciplinary policy setting out the procedures for when employees are working off-site.

In addition to having policies in place, employers should review their employees' contract of employment to take into account that the employee may be working irregular hours given the flexibility of working off-site and ensure that they are tailored for the nature of the work likely to be undertaken. Furthermore, if employees are likely to be developing any intellectual property off-site or at home then specialist intellectual property provisions will need to be inserted to ensure that any past or future intellectual property rights created by employees are assigned to the employer.

Software Patents Update

The difficulty of obtaining patent protection for software is well known. We have previously commented in detail on cases where attempts have been made (some successful) to obtain such patent protection. Given the value of patent protection, to recap, the grounds that need to be established for a “software” patent application to be successful are:

1. the invention must be new;
2. it must involve an inventive step;
3. it must be capable of industrial application; and
4. it must not fall into one of the exclusions contained in Sections 1 (2) or 1 (3) of the Patents Act 1977.

The problems associated with patenting software revolve around the fact that a program for a computer falls firmly into one of the exclusions of the Patents Act.

In a recent case, the Nokia Corporation completed a patent application regarding the developing of mobile phone functionality. The invention uses software elements stored on a smart phone whilst the software developer inputs and creates further software scripts on a computer which are then transferred to the phone and which combine two or more of the software elements stored on the phone, to produce applications. The result of this process is that non computer programming experts can easily change the functionality of the phone and the previous technical problems in doing this are avoided.

The UK Intellectual Property Office allowed the application having reviewed case law, on the basis that the Nokia invention overcame previous technical problems and therefore provided a technical contribution and was not simply a computer program. This recent case confirms the approach taken in *Symbian Limited v Comptroller General*. However, it is interesting to note that in the Nokia case the patent was granted even where the software acts as an interface for other software applications.

The advantages of having a patent are that the owner or software inventor will have an absolute right against any unauthorised use of the software that has been patented. This means that the inventor can stop other people using their invention without their permission. It also means that if any other invention falls within the scope of the patented software then the owner can claim damages or even an injunction to enforce their rights.

Cookies

There are recent developments in relation to the law surrounding cookies to be implemented shortly from an EU Directive that providers and operators of websites need to be aware of when creating and planning websites for their clients.

Currently the law states that websites must inform users if they use cookies and allow the user to opt out. This is normally dealt with by the website's privacy policy which outlines how information is collected, what cookies enable the operator of the website to do and how the user can deactivate cookies. It should be noted that cookies are also currently allowed if they are necessary for the provision of information society services.

The recent amendments to the EU Directive state that cookies will only be allowed if the user has either “given his or her consent, having been provided with clear and comprehensive information” or if the cookie is strictly necessary for the provision of services that have been explicitly requested by the user.

Currently the law does not require advance notice and consent to cookies and it will be interesting to see how the amendments are transposed into national legislation. It may now be that, when the Directive is enacted, website operators will have to ask users for their consent before a cookie is placed on the user's computer. The practical implications of this may be that, if the user has to accept each cookie, it is likely to slow down the operation of the website and the user's experience. It will be necessary to see how the need for consent from the user is interpreted and brought into our legislation.

These changes have to be implemented into law in the UK by 25 May 2011.

IT Team - Key Contacts



Carl Newton
Managing Partner & Head of IT Law

Carl, the firm's Managing Partner, is an experienced company/commercial lawyer with considerable expertise in the IT sector. He is the head of our IT team. Carl has particular expertise in advising on acquisitions and disposals of IT companies and businesses, joint ventures and the financing, exploitation and development of IT and Internet technologies and products. He is a member of the Society for Computers and Law.

carl.newton@neilmyson.co.uk



Tim Norman
Partner

Tim is a partner and is an expert in IT and commercial litigation. He has many years of experience in dealing with disputes, arbitration and court proceedings involving complex IP and IT issues.

tim.norman@neilmyson.co.uk



Carla Murray
Solicitor

Carla is a solicitor in our Company/Commercial Department, specialising in IT, intellectual property and commercial law. She has particular expertise in advising in software licensing, e-commerce law, outsourcing, franchising and data protection matters.

carla.murray@neilmyson.co.uk



Charlotte Gilbert
Solicitor

Charlotte is a solicitor in our Employment Department dealing with all aspects of Employment Law including both contentious and non-contentious matters. Charlotte's expertise includes providing advice on HR and Employment related legal matters both to IT businesses and contractors including advice on status issues, contracts, IP rights, home and out of office working issues, post termination restrictions and employment related disputes.

charlotte.gilbert@neilmyson.co.uk

**NEIL
MYERSON
LLP**

SOLICITORS

Neil Myerson LLP
The Cottages Regent Road
Altrincham Cheshire WA14 1RX

T (0161) 941 4000
F (0161) 941 4411
DX 19865 Altrincham
E lawyers@neilmyson.co.uk
W www.neilmyson.co.uk

For more news and articles,
please visit our **NEW**
WEBSITE -
www.neilmyson.co.uk