INTO THE CLOUD

The use of cloud computing presents undeniable advantages, but the legal risks associated with it should not be overlooked

ON 26 JUNE 2014, the EUROPEAN Commission announced that it had been presented with guidelines on the standardisation of service level agreements (SLAs) for cloud computing services.

The publication of the guidelines represents only the latest step in the Commission's wider European cloud strategy, which was launched in 2012 with the objective of delivering a net gain of 2.5 million new European jobs and an annual boost of €160bn to European GDP by 2020.

The size of the market for cloud services across the EU and the opportunities for growth that the European Commission has identified are indicative of the benefits that cloud services can bring to businesses of all sizes.

There is no single definition of cloud computing services, but in essence, they involve the provision of infrastructure and software services via remote or networked servers over the internet, rather than via local onsite infrastructure and servers.

It is easy to see why the take-up of cloud services has been so high and why the market is predicted to grow at such a rapid rate. With the necessary infrastructure being the responsibility of the cloud service provider (CSP), the customer is spared the maintenance costs, capital expense and IT resource time typically associated with in-house IT projects. Equally, because the infrastructure sits with the CSP, the customer can acquire the necessary resource and capacity as and when it is needed, which can lead to significant efficiency savings.

However, cloud services also bring risks, particularly for businesses with potential exposure to litigation or regulatory investigations, where documents may need to be accessed on a time-sensitive basis and where any failings in document retention could result in significant negative consequences.

This article considers the nature of those risks and the steps that businesses can take to protect themselves in the context of the evolving cloud services market.

Summary of EU guidelines

The Commission's publication of the guidelines for standardisation of SLAs for cloud services is undoubtedly a positive step towards assisting businesses across the EU in managing the risks associated with cloud services. The guidelines have been prepared by a Cloud Select Industry Group, which included major CSPs such as Amazon, Google, Microsoft, Oracle and IBM and international professional service firms, including DLA Piper and PwC.

The guidelines identify the types of objective criteria that should be included within SLAs to enable customers to measure performance. Such criteria include:

- availability levels, CSP response times, support and maintenance commitments and data retention policies;
- security standards, including in respect of service reliability, user authentication, data encryption and security auditing rights;
- data management standards, including in respect of data classification, data mirroring, back-up and restoration policies, data lifecycle and data portability; and
- personal data protection standards, including in respect of data protection compliance, data processing, notification of disclosure requests and limitations on the circumstances in which data can be transferred cross-border.

Users of cloud services within the EU will be better placed to control and monitor risk if the guidelines are adopted by CSPs within their standard form SLAs. The Commission has indicated that it expects that adoption of the guidelines will lead to greater trust in cloud solutions, which, in turn, will lead to increased revenues for CSPs as the market continues to grow.

The objective of generating greater trust in cloud solutions should be also furthered when the proposed EU Data Protection Regulation finally comes into force.

The intention behind that Regulation is to create a single pan-European law for data protection, replacing the current position where, although the EU Data Protection Directive 94/56/EC sets minimum measures for data protection, member states can implement stricter requirements. This results in inconsistencies in national data protection laws and competing provisions applying to services provided across more than one member state.

The particular legal issues that arise in the context of cloud computing can be mitigated against by businesses keen to use it because of the significant commercial advantages that it provides

Risks arising from the use of cloud services in the context of legal proceedings

Although the risk profile of using cloud services across the EU will likely change once the SLA guidelines and the EU Data Protection Regulation are adopted fully, businesses with exposure to litigation and regulatory investigations should be aware of the types of risks that are inherent when using cloud services.

In particular, the varying requirements under the laws of different European jurisdictions in relation to the retention, search for and disclosure or production of documents in the event of domestic or foreign litigation and varying data protection/privacy laws, can all lead to complications in the context of cloud storage solutions.

While typically more of an issue in common law jurisdictions (such as England, where parties to litigation are under a duty to retain and then disclose relevant documents in their control), cloud storage of documents may mean that document disclosure issues can also arise in civil law jurisdictions where obligations to produce documents are typically far more limited.

Particular issues arise in this context in relation to cloud document storage because of the attendant uncertainties concerning the physical location of cloud data. As explained above, cloud storage is usually provided by a third party and located remotely from the business, often in another jurisdiction, in multiple jurisdictions, or even in changing locations. In practice, therefore, a company's data is often divided and stored in different countries and may become subject to the laws of the jurisdiction in which it is stored (for example, where the CSP's servers are located).

This can become problematic because of the varying laws, even across European jurisdictions, in relation to the collection of documents for foreign proceedings. For example, although the search for and collection of data in the control of a party may be mandated by one law, the law of another European country can prohibit the search for or disclosure of documents located in that jurisdiction for use in foreign proceedings.

The English courts considered this issue (although not in the context of cloud services) as recently as last year in *Secretary of State for Health v Servier Laboratories Ltd* [2013] EWCA Civ 1234 and *National Grid Electricity Transmission plc v ABB Ltd* [2013] EWHC 822 (Ch), effectively deciding that documents stored in France must be disclosed notwithstanding that French law gave rise to a risk of prosecution for doing so. Businesses may therefore end up in a position where the use of cloud storage solutions and the requirement to collect documents in the event of litigation exposes them to potential breaches of local laws even where they may not have been aware that their documents were located in the relevant jurisdiction.

Third-party disclosures

Another key risk arising from cloud services in the context of disputes is the possibility of applications for third-party disclosure being made directly against CSPs to compel them to provide documents within their control. This is highly undesirable both for CSPs and customers and leads to the risk of conflicts between the CSP's contractual obligations to customers and legal requirements imposed by, for example, a court order mandating disclosure.

Businesses should also be aware that the cross-border nature of cloud storage could lead to the possibility of governments, law enforcement agencies or regulatory bodies in jurisdictions where data is stored being able to access their documents for the purposes of investigations or surveillance. Generally speaking, in these circumstances (unless the request can be challenged because it does not comply with applicable laws), the CSP will have little option other than to provide access to its customers' documents. Although it has always been the case that governments generally are entitled under national laws to access privately held data in circumstances where national security or serious crime is an issue, cloud users should be particularly aware that the multi-jurisdictional features of cloud storage mean that documents may be susceptible to access by different governments across the world.

The particular legal issues that arise in the context of cloud computing can be mitigated against by businesses keen to use it because of the significant commercial advantages that it provides. Ideally, cloud customers should undertake due diligence into their CSPs at the outset to determine which jurisdictions documents are likely to be stored in and therefore which national laws will be at play. It is also good practice to engage with CSPs about their procedures for dealing with disclosure requests from third parties (whether courts or government/regulatory bodies) to gauge the CSP's awareness of the issues and its processes for considering and responding to such requests.

It is also important for customers to select CSPs that can easily facilitate the preservation of documents in the event of litigation or investigations by implementing the immediate suspension of auto-deletion procedures (thereby preventing possible adverse inferences in the event of the loss of data) and that offer sophisticated search tools that can provide benefits in any litigation or investigation.

Limitations and risks

The use and reach of cloud computing is expanding and, although this is undoubtedly a positive development for businesses across Europe, its limitations and risks should not be overlooked.

Businesses should be cautious when deciding whether to use the technology, the CSP they choose and the extent to which cloud storage is implemented, particularly in light of the difficulties that could arise in the context of document retention, litigation and investigations.

This is particularly relevant as a result of the differing nature of technology and privacy laws across the EU, and, as mentioned above, although steps are now being taken to increase certainty and co-operation between and across states, different interpretations and approaches to disclosure and document retention will continue to cause difficulties for businesses.

However, as long as businesses (especially those operating cross-border) are aware of the issues and have open communication with CSPs, the actual and potential benefits of using cloud computing technology appear to far outweigh the risks.

Phillip Kelly and Elinor Thomas are senior associates at DLA Piper UK