Cloud computing continues to increase in popularity. ‘It’s a long-running trend with a far-out horizon. But among big megatrends, cloud computing is the hardest one to argue with in the long term.’

There are potential advantages for businesses both large and small, in limiting administrative effort and saving costs, by using resources remotely for collection, processing, storage and retrieval with an infrastructure based on the internet, and a service managed by a third party provider.

However, the business model adopted by most cloud computing service providers means that data may be stored and transferred across many jurisdictions. So, amongst the risks to be managed in the use of cloud computing are those of ensuring that personal data – data about any living individual who is identifiable from the data – is processed in compliance with the law. Any business located in the UK – indeed, within the European Union (‘EU’) – is subject to data protection laws, including the eight Data Protection Principles enshrined in the legislation. For further information on these Principles see the ICAEW’s Helpsheet 17 ‘Data Protection Act 1998 and the Accountancy Profession’.

Complying with the UK/EU data protection regime
For compliance with the UK/EU data protection regime, the following issues are particularly relevant in relation to cloud computing:

- Third party access to data beyond its owner’s intentions
- As ‘data controller’, the business is responsible for controlling the personal data it holds and processes
- There must be an effective contract for third party ‘data processors’ who process the personal data on the business’s behalf.

The Information Commissioner’s Office has various powers to enforce the data protection regime in the UK, including the power to fine organisations for serious breaches of the law. Businesses operating in regulated industries such as financial services or healthcare, where sensitive information is held, are subject to more extensive data protection obligations.

Where to start?
The first thing for the business to address is whether personal data needs to be part of the data accessed, stored and used in the cloud computing service.

If so, the two principal considerations which arise are firstly storing and processing the personal data remotely, and secondly, the terms of the relationship between the customer (as data controller) and the cloud service provider (as data processor) respectively.

Cross-border transfers
The principal significance of cloud computing for data protection is that data may be stored and processed ‘somewhere in the cloud’, anywhere, across different jurisdictions. A cloud service provider may use numbers of data centres and sub-contractors, and data may typically be transferred from one jurisdiction to another or to other cloud computing providers. Customers

---

may not know at any point in time where their data resides or who is processing it – and for data other than personal data, may not need to know.

The eighth Data Protection Principle restricts the transfer of personal data outside the European Economic Area (EEA) unless adequate protection can be assured. (The EEA includes all countries in the European Union, together with Iceland, Liechtenstein and Norway.)

It is therefore necessary to ascertain where the processing takes place.

Personal data transferred within the EEA, or to a jurisdiction approved by the EU’s European Commission (Argentina, Canada, Guernsey, Isle of Man, Jersey and Switzerland) has the level of protection required. Some American companies comply with a ‘safe harbor’ scheme, approved by the EU. Beyond these approvals, personal data should be transferred only under arrangements to ensure that the data stays protected.

Normally this is by means of written contract.

In some jurisdictions interception law permits certain law enforcement agencies to access, intercept and seize personal data, for example under anti-terrorism legislation – such as the USA PATRIOT Act, or in the UK the Regulation of Investigatory Powers Act 2000.

The data controller/data processor relationship

In using external providers of any kind, the data controller remains in control of personal data, which must still comply with the Data Protection Principles. The typical relationship between provider and customer for data protection is that the provider will be a data processor under the legislation, and acts only on the instructions of the data controller. (But in certain instances of cloud platform services, the cloud service provider may take decisions on moving the data, access, and security measures, and might then be said to be acting as data controller.)

Data controllers are legally required to enter into proper agreements to meet data protection standards and minimise the risks of data misuse or loss. There are various European Commission-approved standard clauses available for data controllers to use. A written contract is the most effective means for managing and protecting personal data. For cloud computing services, additional specific agreement should be reached over a number of points.

The contract

The cloud service provider should have a data protection policy in place, and be able to demonstrate that its staff, wherever they are, have an informed understanding of the importance of following it.

The contract should address the following requirements of the cloud service provider:

- The cloud service provider’s responsibilities should be described, with assurances that data will be used and
processed only in accordance with the customer’s instructions and the Data Protection Principles, for example not to retain the data for longer than instructed;

- A commitment to adequate technical and organisational security measures to keep the data secure, such as secure business continuity arrangements for serious technological or procedural failures;
- An indemnity for loss of data or unauthorised disclosures;
- An obligation to report any unauthorised access or data loss;
- Regular audit rights by or on behalf of the customer.

Importantly it is the customer’s responsibility to ensure compliance with the eighth Principle, as with the others. Therefore the cloud service provider must be able to offer and agree on specific geographical locations where personal data can legitimately be stored and processed (such as the EU).

Future trends

Both the technology and the law involved are evolving. What may happen in the future?

The European Commission is already actively considering making formal notification of data protection breaches a legal requirement. There are also plans to widen the power to sue under the legislation, to allow interested organisations representing individuals’ interests to do so, since people affected by loss or misuse of their data often do not have the resources or inclination themselves.

International codes of practice could be developed and adopted, to help with compliance outside the EEA.

Many cloud service providers are looking at designing more sophisticated privacy features into their cloud infrastructure, applications, software and services. As time goes on, customers will find a greater choice of cloud service providers who can deal with EU personal data requirements.

Conclusion

The first business priority, as in selecting any supplier, is to choose one who is financially sound, reliable and reputable. The cloud service provider must appreciate the genuine concerns over personal data, and be willing to meet the customer’s requirements in complying with the data protection legislation, and in agreeing the terms of a contract which covers the issues.

The Information Commissioner’s Office has published a personal information online code of practice, about collecting and using personal information online generally. It includes reference to data protection and cloud computing services, and is available at www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf

POINTER TO REMEMBER:

If you are looking to use a cloud computing supplier to provide online accounting services:

- Take care in selecting the cloud provider
- Review whether personal data needs to be included in your requirements
- Remember that you legally remain in control of the personal data
- Ensure that the personal data will be processed within approved jurisdictions
- Enter into a contract with the provider which will meet approved data protection standards.

Glossary of terms used in the context of this article:

**Business using cloud computing service**
- Business
- Customer
- Data owner
- Data controller

**Cloud computing service**
- Provider
- Cloud service provider, third party provider
- Data processor

Rachel Burnett
Head of the IT/IP Department and a Partner at
Paris Smith LLP, Solicitors
E rachel.burnett@parissmith.co.uk