MAYER·BROWN

Article

This article first appeared in a slightly different form in the *Financial Times*, 7 March 2011

CLOUD COMPUTING AND PRIVACY CONCERNS

By Mark Prinsley

Any business contemplating moving its IT operations to a cloud based solution – or as the UK Information Commissioner has called it, internet based computing – must balance the privacy and security risks against the potential benefits offered by cloud computing. The General Counsel of Microsoft is quoted as saying that more than 75% of senior business leaders believe that privacy and security concerns are the most significant risks affecting the adoption of cloud based solutions.

Cloud computing involves a degree of loss of control of data by the customer so that the service provider, and not the customer, makes decisions about how the data is processed. Processing in "the cloud" may involve a complex web of parties processing data in a variety of locations around the world by sub-contractors of the party with whom the customer has contracted.

Where personal data is processed otherwise than simply in accordance with a data controller's instructions or where personal data is transferred to a jurisdiction outside the EU which is not regarded has having an adequate data protection regime, then the data controller triggers additional requirements under EU data protection legislation which was drafted in an era which did not contemplate the technologies now used to deliver cloud computing solutions.

The standards imposed by EU data protection laws will apply to "personal data" processed on the EU even if the personal data originated outside the EU and does not relate to EU citizens. So the use of cloud solutions which involve processing in the EU can bring personal data relating to non EU citizens within the ambit of EU data protection laws.

The EU data protection compliance difficulties for cloud computing solutions have been recognised at both the UK domestic level and at the European level. In the UK, the Information Commissioner's office published its Personal Information Online Code of Practice in July 2010. The Code touches on the use of cloud based solutions such as data storage delivered by third parties. The Code notes that the data controller has obligations to ensure that personal data is protected wherever and by whoever it is processed. It comments that cloud based computing brings with it the prospect of complex chains of contractors and lack of certainty as to who is processing personal data on behalf of the data controller/ customer.

Whilst some practical guidance is offered (which is described below), there is no guidance on compliance with the formal aspects of data protection. There is a risk that by giving the cloud solution supplier discretion as to how personal data is processed, which is to some extent inherent in any cloud based solution, the supplier becomes a data controller and not just a data processor processing personal data in accordance with the data controller/ customer's instructions. The question of whether the supplier is a data controller or a data processor affects the notification of the

Mark Prinsley

Partner and Head of IP and IT
mprinsley@mayerbrown.com

arrangements which must be given to the individual data subjects. The customer is also left with the risk that it may not have put in place appropriate arrangements with entities in non EU countries which may process personal data as part of the cloud solution services.

At the EU level the Commission is consulting on potential reform of data protection laws. In its communication of December 2010 outlining the new challenges for the protection of personal data in Europe the Commission refers specifically to the challenge cloud computing brings to the concepts of data protection as individuals (and data controllers) lose control of potentially sensitive information held on remote servers. The Commission anticipates proposing reform of data protection law in 2011.

In the meantime, businesses contemplating the implementation of a cloud based solution involving processing of personal data should certainly take account of the UK Information Commissioner's guidance in the online data code of practice. This guidance indicates that businesses should take steps to:

- confirm the supplier will only process personal data in accordance with the customer's instructions;
- understand the supplier's ability to recover from technological or procedural failures;
- understand the remedies in the event of loss or corruption of personal data;
- understand the level of assurance given in relation to processing of data in countries with weak data protection regimes.

All these points will be covered in a well drafted services agreement.

Ultimately a key question is the level of confidence given in relation to the security standards to be observed by the service provider. In order to comply with EU personal data requirements the data controller needs to ensure that the security standards are appropriate having regard to the nature of the personal data, the state of technological development and the cost of implementing particular measures. Until there is further guidance from the EU, organisations should consider carefully any guidance produced by industry bodies and trade associations focussed on cloud computing issues for organisations of a similar size and level of sophistication. There will be no one size fits all solution as far as compliance with the security standard is concerned but failure to implement acceptable security standards has the potential to cause significant reputational damage, as it seems senior business leaders recognise.