Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

Volume 12, Number 12 December 2012

Protecting Corporate Data in the Cloud With the Aid of EU and UK Guidance

By Mark Prinsley and Daniel Gallagher, of Mayer Brown International LLP, London.

Reports on cloud computing in 2012 suggest that a large number of businesses are now using at least one cloud-based service. Providers promote cloud services as a means for companies to achieve significant savings on their operations and at the same time giving them the agility to respond quickly to business needs and fluctuating market conditions.

The economies of scale benefit associated with cloud computing assumes a single repository for data being used by many clients. This model raises fundamental concerns around information security and regulatory compliance. As well as ensuring that business-sensitive information stays secure, organisations must meet complex requirements imposed on them by a range of privacy and security laws.

In the European Union, data protection regulators have turned their focus to compliance within the cloud. One of their principal motivations is to see that data protection standards of cloud computing are not lower than those of more conventional forms of data processing. The guidance they have produced can be used by businesses that have already deployed or are considering deploying a cloud service.

This article looks at a number of issues that organisations may consider when deciding whether to transfer operations to a cloud service, and offers some practical suggestions for protecting data in a cloud.

EU Data Protection and Security laws

From a European Union perspective, if a cloud service processes personal data and either the cloud customer is established in an EU member state or the processing takes place within the European Union, then the services will need to meet the requirements of the EU Data Protection Directive (Directive 95/46/EC). Personal data is defined very broadly in the Directive. Therefore, almost all data processing in the cloud will fall under its scope. The cloud client, as data controller, is obliged to comply with local laws implementing the Directive in the member state in which the processing takes place. Other, sector-specific regulations and standards may also apply. For example, financial institutions or businesses carrying out investment activities may also need to comply with the EU Markets in Financial Instruments Directive (MiFID), and, in the United Kingdom, with security requirements of the Financial Services Authority (FSA).

EU and UK Guidance

Help navigating through the complexities of EU data protection law, and the issues that should be considered when securing data in a cloud, can be found in the recent EU Article 29 Data Protection Working Party (WP29) "Opinion on Cloud Computing" (*see*

analysis at WDPR, July 2012, page 8) and in the United Kingdom in the Information Commissioner's Office (ICO) "Guidance on the use of cloud computing" (*see analysis at WDPR, November 2012, page 4*).

The WP29 believe that most of the risks connected to processing data in a cloud arise from a lack of control over the data and a lack of information to cloud clients concerning what processing is taking place. Suggested contractual provisions concentrate on addressing these two underlying issues. The ICO Guidance provides cloud clients with a number of practical approaches to consider in order to make certain that the processing of data in a cloud complies with UK data protection laws. The ICO also emphasises that cloud clients remain responsible for how personal data is processed, even though this service is provided to them through a cloud.

Practical Steps

Risk Analysis

Before moving business-critical data to a cloud, there should be a comprehensive risk analysis of whether the data is actually appropriate to be transferred. Particularly sensitive or business-critical data may not be suitable. The processing of sensitive personal data will require additional safeguards, and the ICO recommends a review of any personal data to be processed in order to determine whether any of it should not be placed in a cloud.

A thorough analysis of the data being transferred to a cloud will help to determine which type of service will be appropriate. Public cloud services achieve economies of scale through shared infrastructure and typically offer standardised services and terms and conditions. This means that prospective cloud users may have to accept limited warranties and indemnities, and will probably have little room to negotiate any additional protections. In contrast, a private cloud service will be provided for a single cloud client only, and there should be greater opportunity to negotiate specific contractual provisions and bespoke arrangements for the processing of data. A private cloud will typically be more suitable for particularly sensitive or business-critical data.

Security Audit

Irrespective of the type of cloud service being considered, it is essential that businesses undertake proper due diligence before signing up and transferring their data. EU data protection law requires data controllers to take appropriate technical and organisational measures to protect data. Prospective cloud clients should not seek to rely solely on contractual provisions to protect critical corporate data. Instead, a thorough, pre-contract investigation of a cloud service should be conducted.

Both the ICO and the WP29 recognise that, in reality, it may be impractical or impossible for a cloud client to physically inspect the premises of a service provider. They suggest that this problem may be overcome where a service provider has arranged for an independent third party to conduct a detailed review of the service provider's security arrangements and provide a copy of this to potential clients, demonstrating compliance with EU data protection obligations. Whilst independent auditing and certification provides a practical solution, the ICO and the WP29 caution that these are not in themselves data protection.

Minimum Contractual Content

There are a number of contractual provisions that a cloud client should look for in its agreement with a service provider. Some of these are necessary in order to adequately protect critical data. Others will be needed to ensure that the cloud client meets its responsibilities as a data controller. A cloud client must, at a minimum: 1) stipulate in the contract that the service provider is to follow the instructions of the client (*i.e.*, data controller) as to how data is processed, and 2) stipulate that the service provider must implement technical and organisational measures to adequately protect personal data.

Security

In order to create greater legal certainty and clearly set out the obligations of the service provider, the contract should specify the concrete technical and organisational measures that the service provider has implemented. The service provider should be obliged to regularly update the cloud client, demonstrating that appropriate security measures remain in place. The ICO recommends that cloud clients seek assurances from service providers that the security arrangements of all sub-processors match those of the cloud provider.

The WP29 recommends that a contract clearly state the extent, manner and specific purpose of any processing of personal data to be undertaken by the service provider. The service provider should be prevented from processing data for any purpose other than that stipulated by a cloud client. In this way, a cloud client retains far greater control over its data. The service provider should also be under an obligation to inform a cloud client of any relevant changes to the service.

Confidentiality

In addition to a well drafted confidentiality clause setting out the obligations of the service provider and its employees, a cloud client should consider obliging the service provider to encrypt personal data. Both the ICO and the WP29 agree that encryption can be a useful way of ensuring confidentiality. Cloud clients should not only oblige the service provider to encrypt personal data that is in transit but also, where appropriate, require the provider to encrypt data that is at rest (*i.e.,* in storage). This is critical where sensitive personal data is being processed.

The WP29 has warned, however, that encryption itself does not render personal data irreversibly anonymous: Even if data is encrypted, the requirements of data protection law still apply. The ICO has recommended that, where encryption is used, cloud users have a policy for management of the encryption key in order to uphold the level of protection encryption provides. The ICO warns that the loss of an encryption key could make data

   ISSN 1473-3579

useless and amounts to the accidental destruction of personal data. This would breach the UK data protection regime.

Access Control

It is important to control who is able to access data. There should be an initial review and ongoing monitoring of access arrangements. The contract should oblige the service provider to carry out security checks on any employees having access to the data. The service provider should also guarantee that it has proper governance of the rights and roles of anyone with access to the data, along with adequate supervision. The ICO recommends that there be a clear policy in place setting out the particular circumstances in which the cloud provider may access the data it processes. This should be monitored, with steps to notify the cloud client if unauthorised access, deletion or modification of data occurs.

Transparency

It is important, from both a data security and a privacy perspective, to know what is being done with data once it is in a cloud. The WP29 recommends that the contract should allow for logging and auditing of processing operations performed by the service provider. The cloud client should also be able to monitor what is being done, and the service provider should be obliged to cooperate. Cooperation should also extend to assisting the cloud client with subject access requests. The service provider should also have a duty to notify the cloud client of any legally binding requests for disclosure and to notify the client immediately of any data breach.

Sub-Processing and Location

It is important to know where and by whom data is being processed. It is quite probable that the service provider may subcontract some activities to sub-processors. It is also likely that a service provider may have computing resources or use sub-processors based in a number of locations inside and outside the European Union.

The EU Data Protection Directive stipulates that personal data may not be transferred to any country outside the European Economic Area unless that country or the recipient provides an adequate level of data protection. Cloud service providers are obliged under the Data Protection Directive to tell clients about any sub-processors they use, including what guarantees sub-processors give to the cloud service provider to comply with EU data protection law.

The ICO recommends that cloud clients request a list of all countries where data may be processed and information about the safeguards in place in those locations. Cloud clients should consider putting in place contractual provisions obliging the service provider to seek consent before engaging any sub-processor. Contractual provisions between the sub-processor and the service provider should mirror those between the service provider and the cloud client. The European Commission has drafted standard contractual clauses which can be used for this purpose. They may also be used for transfers of personal data to locations outside the European Economic Area. The WP29 recommends inserting a provision allowing a cloud client to object to any changes in sub-processing or to terminate the contract.

Data Retention and Deletion

The contract should stipulate exactly what happens to the data when a cloud client withdraws from a service. A cloud client should assess in advance and seek contractual assurances that the service provider will be able to delete all of the data, and copies of it, held in all locations on all of its systems. This is important to ensure the protection of business-critical information. In addition, the EU Data Protection Directive stipulates that personal data should not be retained by a data controller any longer than necessary once processing has ceased.

The EU Article 29 Data Protection Working Party "Opinion on Cloud Computing" can be accessed at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

The UK Information Commissioner's Office "Guidance on the use of cloud computing" can be accessed at http://www.ico.gov.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx.

Mark Prinsley is a Partner and Head of the IP practice, and Daniel Gallagher is an Associate in the IP practice, at Mayer Brown International LLP, London. They may be contacted at mprinsley@mayerbrown.com and dgallagher@mayerbrown.com.