EU Data Protection Regulators and Cloud Computing Contracts

By Fiona Wilson and Oliver Bray

The recent rise of cloud computing – both for businesses and at consumer level—is providing a decent challenge for the regulators tasked with applying established data protection principles to this new, and fast-developing, industry. Until recently there has been little guidance from the United Kingdom (UK) or the European Union (EU) regulators. However, in July 2012, the Article 29 Working Party (WP) – the independent advisory body made up of data protection regulators from across the EU member states—released its Opinion 05/2012 on Cloud Computing (the Opinion). This was closely followed by guidance from the UK regulator, the Information Commissioner's Office (ICO). The ICO's Guidance on the use of Cloud Computing was published at the end of September 2012 (the Guidance).

The WP and ICO have attempted to provide workable and commercial solutions for both cloud suppliers and their customers. Both regulators conclude that data protection legislation should not be a bar to using cloud services but certain measures must be put in place, mainly by the customer, to ensure compliance with the data protection principles at each stage of the cloud chain. Helpfully, the Guidance includes a practical checklist of issues to consider when using the cloud for personal data.

This article looks to these documents for the key considerations for both suppliers and customers looking to use cloud arrangements for personal data.

Fiona Wilson *is an associate and* ***Oliver Bray*** *is a partner in the Intellectual Property area at RPC LLP. Oliver heads up RPC's data protection practice in London. He is a recognised specialist in digital media and is ranked as a leading commercial lawyer ("Tier 1") in the UK Legal 500 directory. Oliver's other specialisms include IP, technology, branding and marketing. Oliver regularly advises his clients on pan-European data protection compliance and data protection strategies including data collection campaigns (oliver.bray@rpc.co.uk). Fiona specialises in commercial contract matters with a particular focus on data protection and e-commerce. She advises on a broad range of technology matters including data protection policies and cookie law compliance (fiona.wilson@rpc.co.uk).*

BACKGROUND

Cloud computing services are now widely available both in the private cloud (where the cloud customer is the sole user of the service) and in the community, public or hybrid cloud (where the cloud is made available to more than one customer). The ICO defines cloud services as "*access to computing resources, on demand via a network*." It is the linked network nature of such arrangements which has particular data protection risks andbecause there is usually a complex outsourcing chain which may span several jurisdictions (noting that many of the leading cloud providers are based in the US). The relevant legal framework in the EU is the Data Protection Directive (95/46/EC) (the Directive) implemented in the UK as the Data Protection Act 1998.

Responsibility for processing of personal data is divided into two categories: that of data controller and data processor. The data controller is the entity which alone or jointly determines the purpose and means of processing and the data processor is the entity which processes personal data on behalf of the data controller.

In the typical cloud computing scenario, the WP and ICO agree that it is the customer who is most likely to have the central data controller role (as it determines the purposes of the processing), and therefore the primary responsibility for ensuring compliance with data protection legislation.

THE WP'S CONCERNS

The WP highlights availability, integrity and confidentiality of data as the key principles to apply in relation to processing personal data in the cloud. Further, the more "*specific data protection goals of*

A utilização deste artigo é exclusiva para fins educacionais.

transparency, isolation, intervenability, accountability and portability to substantiate the individual's right to data protection" also come into play.

The Opinion highlights a lack of control and a lack of transparency for the customer as a matter of serious concern. A customer can only take responsibility for data protection laws if it is actually aware of the risks and threats. If a customer has insufficient information about the supplier's processing operations (for example, its use of any sub-processors, transfers outside the client's jurisdiction, etc.) this will prevent the customer being able to assess the risks and take appropriate steps to mitigate them.

The WP believes the key to protecting personal data in the cloud is the contractual document between the parties, not least because the law requires a written contract for data processing.

THE WP'S SUGGESTED SOLUTIONS

The WP makes it clear that compliance with data protection rules and responsibilities (including in the event of a breach) must be clearly allocated between the parties in the contract. Although the customer, as data controller, has the main compliance burden, the supplier is not off the hook. The WP says that "*cloud providers should provide documentary evidence of appropriate and effective measures that deliver the outcomes of the data protection principles*."

The Opinion includes a list of issues which the WP suggests should be addressed in each contract, such as:

- full details of the customer's instructions for processing personal data including the extent, manner and purpose of processing and the nature of the data;
- detailed specifications of the data security measures for processing personal data;
- conditions for returning or destroying personal data on expiry or termination of the contract;
- confidentiality;
- obligations for the supplier to cooperate with the customer in any data subject access requests;
- no right of disclosure to any third parties (including sub-processing) without the customer's consent; and
- division of responsibilities in the event of a data breach—with contractual penalties/remedies (including proportionate and effective service credits).

The Opinion also recommends including a list of locations where the data may be processed and appropriate clauses for transferring personal data outside the European Economic Area (EEA). The Directive only allows data controllers to transfer personal data to countries outside the EEA that adequately protect the data or if the data controller has put in place approved safeguards. In the European Commission's cloud strategy: "*Unleashing the Potential of Cloud Computing in Europe*," (September 2012) the Commission proposes to review the current standard contractual clauses for international data transfers and make them more cloud-friendly.

The WP does recognise that this type of service (at both corporate and consumer level) is often offered up on the basis of a supplier's standard terms for which there is not much "*room for manoeuvre*." The WP then makes it clear that an imbalance in power "*should not be considered as justification for the controllers to accept clauses and terms of contracts which are not in compliance with data protection law*." Each cloud contract should, therefore, take note of the above.

THE ICO GUIDANCE – KEY CONSIDERATIONS

In a similar manner to the WP, the ICO highlights and explains the new data protection risks a customer must consider as a result of putting personal data in the cloud. The ICO spells out to companies that responsibility for data protection compliance generally remains with the customer (as data controller) even when data physically passes to the supplier. The division of responsibility will need to be considered on a case by case basis depending on the type of cloud arrangement, albeit the ICO states that "*the cloud customer will generally be a data controller - and therefore ultimately liable for compliance*."

Like the Opinion, the Guidance is also based on the key principles of availability, confidentiality and integrity and explains what a customer should consider when looking to engage a supplier in relation to each of these principles. The ICO's checklist summarises the practical steps for business to consider to avoid falling foul of the rules. This starts with the ICO advising

A utilização desta obra é exclusiva para fins educacionais

the customer to prepare a list of the personal data it intends to place in the cloud and, from there, assess the processing risks. This broadly covers the same areas as the Opinion and also includes consideration of:

- measures to prevent unauthorised access to data including a system to create, update, suspend or delete user accounts;
- policies to delete all copies of personal data as may be required by the customer;
- procedures for dealing with personal data on expiry or termination of the contract;
- policies to allow customers to have access to their personal data;
- audit processes for any authorised access, deletion or modification of personal data;
- full details of where personal data will be processed and how it will be processed; and
- details of back-up procedures.

Like the Opinion, the Guidance also reminds customers of their other legal obligation such as to have written contractual measures for safeguarding transfer of data to other countries and to protect the rights and freedoms of data subjects. Once a customer has assessed the risks, it is then in a better position to introduce measures to mitigate them.

The ICO warns that this should not be seen as a static list. It recommends a continual cycle of monitoring, review and assessment to ensure that the service is being provided in accordance with the agreed contract. The ICO recognises that many of the above considerations rely on disclosure of information from the supplier or from site audits on the premises where personal data will be processed. As a result, the ICO also suggests that a supplier arranges for an independent third party to conduct a detailed security audit of its service to check for appropriate technical and organisational measures (as is required by the Directive). This report can then be provided to each of its customers and would avoid the need for each customer to conduct a separate review each time. The ICO also supports the introduction of an industry recognised standard or kitemark to assist cloud customers (in particularly, the consumer) in assessing the security offered.

COMMENT

Both the WP and the ICO place the burden of data protection compliance very much on the shoulders of the customer. On this basis, a supplier should be carefully selected for guarantees for data protection compliance. One message that is very clear is that it will be no excuse to the regulators that a provider's non-compliant standard terms are the only contractual terms on the cards.

For new cloud services, the customer should conduct a full due diligence examination prior to entering into any arrangement. The results of this risk analysis should be captured in the contractual documents between the parties; the extent of the clauses will depend on the nature and risk of data being placed in the cloud.

For existing services, suppliers and their customers should carefully review their current contractual terms and conditions (including standard terms) and adapt their practices in line with this new guidance.

Both regulators recognise that the complexities of the cloud computing arrangement cannot be wholly addressed using the measures identified in these documents. However, their guidance is welcomed to both highlight the potential issues and provide practical tips for the processing of personal data by suppliers in the EEA. Neither the Opinion nor the Guidance has the force of law but the regulators will be expecting companies to comply with these rules and each party should now be better equipped to understand what the regulator wants from them. The onus now lies with the suppliers, customers and their advisors to put the theory into practice.

A utilização deste artigo é exclusiva para fins educacionais.

Copyright of Journal of Internet Law is the property of Aspen Publishers Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.

Fonte: Journal of Internet Law, Vol. 16, Issue 8, p18-20. 3p. Feb. 2013 [Base de Dados]. Disponível em: <http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=dde43605-dbd9-40aa-99f8-20ad0f1d7625%40sessionmgr110&vid=4&hid=126>. Acesso em: 1 Mar. 2013.

A utilização deste artigo é exclusiva para fins educacionais.