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 11 November 2012

The UK Information Commissioner's Office Guidance on the Use of Cloud Computing

By Renzo Marchini and Ed Holmes, of Dechert LLP, London. Renzo Marchini is a member of the World Data Protection Report Editorial Board and the author of "Cloud Computing: A Practical Introduction to the Legal Issues".

Introduction

In July of this year, the EU Article 29 Data Protection Working Party published its guidance on the use of cloud computing[1] (*see analysis at WDPR, July 2012, page 8*). The UK Information Commissioner's Office ("ICO") followed this in late September 2012 with a paper which, in substance, is similar, but, as is usual with the publications of the ICO, is presented in a much more "user-friendly" manner. The ICO is pragmatic, and, whilst the document offers guidance and warnings, it is not by any means proscriptive.

This will be particularly refreshing for the cloud industry, providers and potential customers alike, as it arrives at a time when regulators in other EU member states have been issuing warning bells on cloud take-up. In February 2011, the Danish data protection agency rejected Odense Municipality's application to use the cloud service "Google Apps" to store data in relation to its public schools (*see analysis at WDPR, April 2011, page 13*). Although it was Google in Ireland that was the initial transferee, since Google in fact stores all its data in numerous data centres worldwide, including in the United States and Europe, the application was refused. In the Netherlands, in September 2011, government departments were severely restricted in using such providers to process government IT data, on the ground that the U.S. "PATRIOT Act" requires U.S. companies to provide data to U.S. law enforcement agencies.

Who Is the Data Controller?

In any analysis of data protection implications in an activity, a starting point is to identify which of various parties is the data controller. It is, of course, the data controller that has ultimate responsibility for compliance with the data protection rules, set out in the UK Data Protection Act 1998. A data controller is the person who determines the purposes for which, and the manner in which, any personal data are to be processed. At present, many cloud providers would argue that they would be considered to be processors, and thus avoid those obligations placed on the controller only. Nonetheless, following the Article 29 Working Party's opinion on the SWIFT case[2] and its subsequent opinion on the "controller" and "processor" definitions[3] (*see analysis at WDPR, April 2010, page 4*), it has not been

possible to be absolutely certain that this will be the case in the eyes of regulators and enforcement agencies.

The ICO guidance is helpful on this aspect. In a cloud computing scenario, it says, the cloud customer will determine the purposes for which, and the manner in which, any personal data are being processed. Therefore, the cloud customer will, in the words of the ICO, "most likely" be the data controller, and thus the party with overall responsibility for compliance with the Data Protection Act.

The guidance dispels the myths that diligence necessitates a physical inspection of the data centre, and that the possibility that foreign law enforcement agencies might get access to data should prevent cloud use.

Having said this, the guidance notes state that the precise role of the cloud provider will have to be reviewed in each case, in order to assess whether or not it is processing personal data and, if so, whether it is merely acting as a "data processor" on behalf of the controller, or whether it is a data controller in its own right. If a cloud provider, for example, were to undertake an activity such as concerned the Dutch authorities (as mentioned above), one of the factors indeed which featured in the SWIFT case analysis that SWIFT was a data controller (although the supply to law enforcement in this latter case was not on U.S. PATRIOT Act grounds), would that make the provider a "controller" in its own right? This issue is not addressed. Nonetheless, UK-based cloud providers will no doubt take comfort from the assessment of the ICO as to what would normally be the case.

Initial Considerations for Data Controllers

Having identified the data controller, the guidance highlights various compliance requirements associated with the use of cloud computing. Many of the data protection issues will, of course, be familiar to data controllers that have outsourced any type of data handling, and are simply applications of well-known principles to a cloud situation. The topics range from giving advice to cloud users ("cloud customers" in the guidance) on being careful in selecting what data to entrust to a cloud provider, to giving advice on putting a written contract in place (a well-known consequences of the seventh data protection principle or Article 17 of the EU Data Protection Directive (Directive 95/46/EC)).

On the latter point, according to the ICO, the provider should not be able to change the terms of the data processing operations without the cloud customer's agreement. In particular, the guidance notes state that cloud customers should take care if a cloud provider offers a "take it or leave it" set of terms and conditions without the need or opportunity for negotiation.

However, the cloud model is predicated on a consistency of service provision for multiple customers on the same or similar terms — with any provider being reluctant to negotiate its standard terms, except for its largest customers.

Security

Security, of course, is one of the biggest concerns with cloud use, even when the cloud service is not processing personal data. The Data Protection Act (as does the Data Protection Directive) requires appropriate security measures in place and an element of diligence in the provider's security standards. In this respect, the ICO guidance helpfully dispels a myth that has plagued a faster general take-up of cloud computing. It is not the case, confirms the guidance, that a physical inspection of the cloud provider is necessary as part of the security assessment. Instead, the guidance suggests that the most effective way for cloud providers to have their security assessed may be for an independent third party to conduct a detailed security audit, the results of which can be provided to multiple prospective cloud customers. Many cloud providers do, in fact, assert certification to the ISO 27000 series of standard, which is a real measure of commitment by a provider.

Perhaps with a touch of wishful thinking, the guidance expressly supports the introduction of a specific cloud industry standard or Kitemark, which would allow cloud customers to compare services offered by cloud providers.

Transfers out of the European Union

Much of the adverse commentary relating to the ability of EU customers to use cloud services is based on an assessment that the United States (where many cloud providers are located) does not provide an "adequate" level of protection for personal data, as required by the eighth data protection principle (Article 25 of the Data Protection Directive).

According to the ICO, cloud customers will, therefore, need to ascertain from the cloud provider details of where the data are to be processed and what safeguards are in place in each different location. Furthermore, the cloud provider should be able to explain when data will be transferred to those locations. Many, if not all, of the major cloud providers are increasingly giving assurances in relation to the geographical locations of data, in particular, that the data will stay in particular regions, such as the European Union. It is always an important conversation to be had.

Here, the ICO helpfully dispels another common concern of potential UK customers: access to data by foreign law enforcement agencies (the U.S. PATRIOT Act is often mentioned in this context). The possibility of this happening is no reason not to use a cloud service, confirms the guidance. Regulatory action would not be taken, for example, against the cloud customer if its U.S. provider disclosed data when legally compelled to do so by U.S. authorities.

  WDPR ISSN 1473-3579

Other Points

The ICO guidance deals with a number of other issues to be considered, such as requirements to make sure appropriate (tailored) training in relation to security is put in place for staff and a reminder to consider encryption for data in transit as well as in rest. Another example is to remind cloud customers that their obligations to safeguard data subject rights (such as subject access and deletion obligations) remain in place, and so the cloud service should allow full compliance.

Conclusion

Much of the guidance repeats good commercial practice (the need to be diligent in relation to security, including controls on what the provider can do with your data, and so on). In other places, however, the guidance contains helpful comments dealing with some of the perceived hindrances to cloud take-up. These include dispelling the myths that diligence necessitates a physical inspection of the data centre, and that the possibility that foreign law enforcement agencies might get access to data should prevent cloud use. That is not the case, as the guidance makes clear.

NOTES

[1] Opinion 05/2012 on cloud computing of July 1, 2012, WP 196.

[2] Opinion 10/2006 of November 22, 2006, on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128.

[3] Opinion 1/2010 on the concepts of "controller" and "processor", WP 169 of February 16, 2010.

The text of the UK ICO's guidance on 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.

Renzo Marchini is Counsel and Ed Holmes is an Associate in the London office of Dechert LLP. Renzo Marchini is a member of the World Data Protection Report Editorial Board and the author of "Cloud Computing: A Practical Introduction to the Legal Issues". The authors may be contacted at renzo.marchini@dechert.com and ed.holmes@dechert.com.