SQUIRE SANDERS

ARTICLE 29 WORKING PARTY OPINION ON CLOUD COMPUTING

An expression of caution but a flexible future

On 1 July 2012, the Article 29 Working Party[1] ("Working Party") adopted an Opinion on cloud computing (the "Opinion"). The Opinion addresses the challenges presented by wide scale deployment of cloud computing services and provides guidance on security requirements, placing a special emphasis "on the contractual arrangements that should regulate the relationship between a controller and a processor." The Working Party also expresses doubt over the effectiveness of Safe Harbor principles and encourages cloud clients to review existing arrangements.

The Risks

The Opinion highlights two main data protection risks associated with the use of cloud services:

1. A lack of control over personal data including:
    - a lack of availability of data;
    - a lack of confidentiality in terms of law enforcement requests made directly to a cloud provider; and
    - a lack of "intervenability" required to assist with data subjects' rights to access, correct or delete their data.

2. A lack of information on data processing as a result of:
    - chain processing involving multiple processors and subcontractors;
    - processing in different geographic locations within the European Economic Area (EEA); and
    - transfers of data to third countries outside of the EEA which do not provide an adequate level of data protection.

1 The "Article 29 Working Party" (named after the provision in the directive that created it) is an independent advisory body composed of representatives of national and EU data protection authorities and of the European Commission. Its opinions are not binding, but enjoy significant authority.

Risk Analysis

The Working Party recommends that, as a first step, a comprehensive and thorough risk analysis should be carried out by those wishing to use cloud services, and notes that the processing of sensitive data requires additional safeguards. The Opinion also includes a checklist for ensuring compliance with data protection principles and endorses third-party data protection certificates as a means of demonstrating compliance.

Contractual Safeguards

The Opinion advocates that cloud clients must choose a cloud provider that will guarantee compliance with the applicable laws, and goes on to say that in order to ensure legal certainty, the following issues, amongst others, should be set forth in any formal contract with a cloud provider:

- The extent and modalities of the client's instructions must be clearly defined including details of the penalties for the cloud provider in the case of non-compliance;
- The cloud provider must adopt security measures in line with the laws of both the controller's and the processor's jurisdictions;
- Cloud providers can only subcontract certain services after having obtained the client's consent;
- Inclusion of a confidentiality clause, binding both upon the cloud provider and any of its employees;
- Obligation to support the client in facilitating the exercise of data subjects' rights to access, correct or delete their data;
- Specification of the conditions for returning or destroying the data once the service is concluded;
- Obligation on the cloud provider to provide a list of locations in which the data may be processed;
- Provision for logging and auditing of relevant processing operations performed by the cloud provider or subcontractors;
- Notifying the cloud client about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited; and
- Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any data breach affecting the cloud client's data.

General Data Protection Requirements

The Working Party reaffirms the basic data protection principles that must be adhered to by both the cloud provider and the cloud client, namely transparency regarding the data subject, purpose specification and limitation, erasure of data, technical and organisational measures of data protection and data security, the provision of timely and reliable access to personal data, integrity of the data, confidentiality, isolation of data, "intervenability", portability and accountability.

International Transfers

"In the view of the Working Party, sole self-certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment." Indeed, the Opinion identifies "several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures, which are not sufficiently addressed by the existing Safe Harbor principles".

The Opinion suggests that companies engaged in transfers of data between the EEA and the US should, at an absolute minimum, review their existing arrangements and investigate implementation of the Safe Harbor principles in practice, with a view to complementing the principles with additional safeguards.

In effect, the Opinion rejects the Safe Harbor mechanism as a transfer solution on the basis that Safe Harbor certification alone cannot substitute for the relevant contractual arrangements and guarantees which may be required by individual data protection authorities.

The Opinion favours the use of the 2010 Model Clauses (with their applicable sub-processor provisions) but more importantly recognises the suitability of the BCR framework and, specifically, the on-going development of Binding Safe Processor Rules (BSPR) which would allow a cloud client to entrust their data to the cloud service provider while being assured that onward transfers for sub-processing purposes would receive an adequate level of protection.

The Way Forward

"Like any evolutionary process, the rise of cloud computing as a global technological paradigm represents a challenge." Whilst acknowledging the significant growth in this area and consequently the need for flexible mechanisms, the Opinion expresses notable caution for data processed in the cloud. It could be argued that the Working Party's expectations are unrealistic and have placed European cloud clients in an unenviable position. However, any move away from onerous contractual requirements towards a more outcome-focused solution should be welcomed and the Working Party's recognition of BSPR as the future model to ensure compliance should be seen as a step in the right direction.

In this regard, the Opinion somewhat mirrors Digital Agenda Commissioner Neelie Kroes' recent call for the creation of an EU-wide strategy for cloud services which, inter alia, provides for a single set of rules valid across the EU and the creation of an EU-wide certification scheme for data protection and privacy in cloud computing.

The Opinion builds on similar guidance issued by the French, German and Italian data protection authorities over the past year. Please see our recent Client Alert on Guidance issued by the CNIL, the French Data Protection Authority:

http://www.squiresanders.com/pdf/CNIL-Guidance.pdf

For more information or if you would like to discuss any of the issues raised in the Opinion, please contact either:

Ann LaFrance
Partner, London
T +44 207 655 1752
E ann.lafrance@squiresanders.com

Dr. Annette Demmel
Partner, Berlin
T +49 30 726 16 8226
E annette.demmel@squiresanders.com

Stéphanie Faber
Of Counsel, Paris
T +33 1 5383 7400
E stephanie.faber@squiresanders.com

7224/07/12