ReedSmith

Client Alert

Global Regulatory Enforcement

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Cynthia O'Donoghue
Partner, London
+44 (0)20 3116 3494
codonoghue@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

Article 29 Working Party Issues Opinion on Cloud Computing

The Article 29 Working Party, which is made up of each of the EU member states' national data protection authorities, issued an Opinion on cloud computing earlier this month. The Working Party acknowledges that for certain businesses, cloud computing has been an important technological revolution and a key area of development for their technology and computing strategy. The Working Party supports the development of cloud computing and its ability to generate economic benefits to businesses and organisations, given the wide range of cloud services on offer and business demand. The Working Party supports the idea of a European Cloud Partnership strategy in favour of public sector procurement of cloud services, so long as special precautions are taken, especially if it simulates development of the European cloud market.

The Opinion analyses the applicable law and obligations for data controllers located in the European Economic Area ("EEA"), for cloud service providers with clients in the EEA, and the applicable principles for both data controller and data processor arising out of the principles in the Data Protection Directive 95/46/EC (the "Directive").

Data Protection Risks of Cloud Computing The Working Party focused on the specific risks related to processing personal data when data is put in the cloud. The majority of these risks fall into two categories: (i) lack of control over the data, and (ii) insufficient information about the data processing operations (lack of transparency).

A. Lack of control

The Working Party notes that when a business enters into a contract which involves committing personal data to the cloud, the business (or cloud client) may no longer be in exclusive control of this data, and will not then be able to deploy the necessary measures to protect the data. This lack of control may manifest itself in the following ways:

- *Portability:* Controllers may find it difficult to migrate data between different cloud-based systems (data portability) or to exchange information with entities that use cloud services managed by different providers (interoperability).
- *Integrity:* The potential for a conflict among shared systems and infrastructures, given the processing of personal data from a wide range of data subjects and organisations.
- *Confidentiality:* Personal data may be subject to law enforcement requests from law enforcement agencies of the EU Member States and from third countries, and may be disclosed by the cloud provider without a valid EU reason.
- *Ability to Intervene:* An inability on the part of the customer to intervene in how the data is processed because of a highly complex and dynamic outsourcing chain.
- *Access:* A cloud provider may not be willing to provide the necessary measures and tools to assist the controller with a data subject request.
- *Inter-linking:* The ability of a cloud provider to use its control over data from different clients to link personal data, rather than ensuring isolation of data among its customers.

B. Lack of information on processing (transparency)

The Opinion raises concerns that controllers may not have enough information about a cloud service provider's processing of data, which could pose risks to both the controller and to individuals, because they might not be fully aware of risks until after they have arisen. If transparent information is provided, however, steps can be taken to stop risks or seek to prevent them from arising.

Potential threats may arise from the controller not being aware that:

- Chain processing is taking place
- Personal data is processed in different geographic locations within the EEA
- Personal data is transferred to third countries outside the EEA

Applicable Legal Framework While the Directive is the relevant legal framework for cloud computing services procured within the EEA where personal data are being processed, ePrivacy Directive 2002/58/EC (as revised by 2009/136/EC) may also apply if telecoms operators or public communications networks provide a cloud solution. In each case, however, it will be the national implementing legislation of controllers of these Directives that will govern the processing of personal data.

Duties and Responsibilities of the Key Players Cloud computing involves a range of players, and the Working Party believes it is important that the roles of these players and their obligations are clear. In the relationship between the cloud client and the cloud services provider, the cloud client (the business) is the data controller as it determines the purpose of the processing and has the ability to delegate the processing to another organisation. The data controller takes the responsibility for abiding by data protection legislation and all the relevant duties in the Directive. The cloud service provider will be data processor as it supplies the means and the platform for processing the data on behalf of the data controller. Processors have a responsibility of confidentiality and must make sure the appropriate security measures are in place. There could be situations where a cloud service provider would be considered as a joint controller or as a controller in its own right. It is clear that no matter how complex the data processing circumstances and relationships, the Working Party wants to see that compliance with data protection rules and responsibilities has been clearly allocated to the parties in the relationship, so that there are no gaps in protecting the personal data.

Businesses should choose a cloud provider that guarantees compliance with data protection legislation and provides a set of data protection safeguards in the contract, even where there is little scope to negotiate terms.

Using the cloud may also involve a number of other parties who act as processors or subcontractors who will have access to personal data. Where services have been subcontracted out, the client should be informed and provided with information regarding the subcontractor, and a guarantee that the subcontractor will comply with the Directive. This means that any contract between the cloud provider and a subcontractor must contain all relevant obligations and must reflect the contract between cloud client and cloud provider. The Working Party comments that subcontracting of activities should only occur with the consent of the controller.

Data Protection Requirements The lawfulness of the processing of personal data in cloud computing will depend on the parties involved adhering to basic principles of European data protection law, such as:

- *Transparency:* Of key importance for fair and legitimate processing of the personal data, as well as in the relationship between the parties.
- *Purpose specification and limitation:* Data must be collected for specified, explicit and legitimate purposes, and not further processed by the cloud client in a way for other purposes that are not compatible with the original ones.
- *Erasure of data:* Personal data should not be kept for longer than is necessary for the purposes, and when it is not necessary any more, must be erased or truly anonymised.

Recommended Contractual Safeguards As well as ensuring that a cloud provider gives sufficient guarantees in respect of technical security and organisational measures, and complies with the Directive, the parties involved are legally obliged to sign a formal contract to govern the relationship. As a minimum, the contract should establish that that the processor must follow the controller's instructions and that the processor must implement adequate measures to protect the personal data. To ensure legal certainty, the contract should also address the following issues:

- Details on the cloud client's instructions to the provider, with particular attention on applicable SLAs and the relevant penalties.
- Specification of security measures that the cloud provider must comply with, depending on the risks represented by the processing and the nature of the data to be protected.
- Subject, time frame and details of processing of personal data of the cloud service to be provided by the cloud provider.
- Details of the conditions for returning or destroying the data once the service is concluded.
- Inclusion of a binding confidentiality clause.
- Obligation on the provider to support the client in relation to data subjects' rights to access, correct or delete their data.
- The contract should expressly establish that the cloud provider may not communicate the data to third parties unless they are approved subcontractors. The contract should specify that subprocessors may only be commissioned on the basis of consent. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned, and guarantee that both cloud provider and all subcontractors shall act only on the cloud client's instructions. The chain of liability should be clearly set in the contract.
- Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any data breach.
- Obligation on the cloud provider to provide the locations where the data may be processed.
- The contract should contain a clause detailing the controller's monitoring rights.
- A clause stating the cloud provider must inform the client of any relevant changes.
- The contract should provide for logging and auditing of relevant processing operations.

- Notification of cloud client regarding any legally binding request for disclosure of the personal data by law.
- A general obligation on the provider's part stating that data processing arrangements are compliant with the applicable legal requirements and standards.

Technical and Organisational Measures of Data Protection and Data Security Under the Directive, the full responsibility lies on cloud clients, as data controllers, to choose a cloud provider that implements adequate technical and organisational security measures to protect personal data. In addition to the core security and data protection goals below, the Working Party states that data controllers should consider the complementary data protection goals of transparency, isolation of data, the ability to intervene, accountability and data portability.

- *Availability:* Such as ensuring timely and reliable access to personal data which could be affected through accidental loss of network connectivity. Cloud clients should check to make sure reasonable backup measures are in place.
- *Integrity:* Such as making sure the data is authentic and has not been altered during processing, storage or transmission in the cloud. Detecting alterations to personal data can be achieved through authentication mechanisms or use of intrusion detection or prevention systems. The Working Party has highlighted integrity of the data as especially important because the cloud will usually operate in open network environments.
- *Confidentiality:* Personal data should be encrypted in all cases when "in transit" and "at rest", as well as the communications between cloud provider and client. Further technical measures should be considered, such as authorisation mechanisms and strong authentication.

International Transfers The transfer of personal data to countries outside the EEA is permitted under the Directive only if there is an adequate level of protection. If not, specific safeguards must be put in place by the controller and/or processors. As cloud computing is normally based on a lack of any stable location of data within the cloud provider's network, this means that the cloud client may not know in real time where the data are located, stored or transferred. Therefore, the traditional legal instruments that are normally used to regulate data transfers to non-EU third countries without adequate protection have limitations in relation to cloud computing. For example:

- Safe Harbor: Limited in terms of geographical scope and may not be sufficient for use in the cloud environment. The Working Party states that companies exporting data should not simply rely on the data importer claiming to have a Safe Harbor certification, and that the Safe Harbor principles alone may not guarantee that the appropriate security measures are in place in the United States.

- Exemptions: The Working Party previously stated that the Directive exemptions shall only apply where transfer of data is not recurrent, massive or structural.
- Model clauses: These Working Party states can be used between the processor and the controller in a cloud computing environment.

Conclusions and Guidelines The Working Party recommends that businesses planning to use cloud computing conduct a comprehensive and thorough risk analysis that seeks to highlight any risks of processing data in the cloud and address them. The list of conclusions in the Opinion are intended to act as a checklist for data protection compliance, such as:

- Assess whether the relationship between the parties is a "controller-processor" relationship.
- The cloud client should be aware of its responsibility as a controller and that it accepts responsibility for abiding by data protection obligations. In light of this, the client should select a cloud provider that guarantees compliance with EU data protection legislation..
- The appropriate subcontracting safeguards should be provided for in the contract.
- The parties should ensure compliance with fundamental data protection principles of transparency, purpose specification and limitation, and data retention.
- Generally, the contract between the cloud client and provider should afford sufficient contractual safeguards in terms of technical security and organizational measures, and should be in writing. The contract should detail the client's instructions, access to and disclosure of data, the provider's obligations to cooperate, and how cross-border transfers will be dealt with.

Recommendations In conclusion, the Working Party highlights some issues that need to be tackled to enhance the safeguards and to assist the cloud industry. The Working Party would like to see a better balance of responsibilities between controllers and processors in light of the new draft Data Protection Regulation, and stressed that it is very important that access to personal data for national security and law enforcement purposes is limited. Controllers operating in the EU are prohibited from disclosing personal data to a third country even if requested by a judicial or administrative authority, unless expressly authorised by an international agreement or treaty, or approved by that controller's national legal system.

ReedSmith