Bloomberg BNA

Privacy and Security Law Report®

Tempest in Cloud Computing Market: Will EU Article 29 Working Party's Opinion Force a Rethink of the Safe Harbor Principles?

BY FRANÇOISE GILBERT

In its Opinion 05/2012 on Cloud Computing (Opinion),[1] published July 2 as document WP 196, the Article 29 Working Party analyzes the applicable data protection laws and obligations for companies providing or using cloud computing services in the European Economic Area (EEA). The Opinion identifies data protection risks that are likely to result from the use of cloud computing services, such as lack of control over personal data and lack of information about how, where, and by whom the data are being processed or sub-processed in the cloud. It also stresses the importance of informing data subjects about who processes their data, for what purposes, and in which locations, and how they can exercise the rights afforded to them in this respect when their data are hosted or processed in the cloud.

[1] "Opinion 05/2012 on Cloud Computing" is available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (11 PVLR 1097, 7/9/12).

Françoise Gilbert is the managing director of the IT Law Group, a niche law firm that focuses on information privacy & security and cloud computing. She serves as General Counsel of the Cloud Security Alliance and as a board member of the International Technology Law Association. She can be reached at (650) 804-1235 and fgilbert@itlawgroup.com.

The Opinion examines the issues associated with the sharing of resources with other parties, the lack of transparency of outsourcing chains with multiple cloud processors and subcontractors, and the transfer of personal data to cloud providers established out of the EEA. In this regard, the most significant aspect of the Opinion is its negative evaluation of the ability of the Safe Harbor self-certification to meet the requirements of the national laws implementing the 1995 European Union Data Protection Directive. The Article 29 Working Party thinks that the loss of governance, insufficient audit trails, insecure or incomplete data deletion are not sufficiently addressed in the existing Safe Harbor principles to provide adequate assurance that the necessary security measures are met.

Scope of WP 196

Most of the recommendations provided in WP 196 focus on the client-provider relationship as a controller-processor relationship. However, the Opinion recognizes that in some circumstances, the cloud provider may act as a data controller as well. In such a case, the Opinion stresses that the cloud provider has full responsibility (or possibly, joint responsibility) for the processing and must fulfill all legal obligations that are stipulated under applicable national laws derived from Directives 95/46/EC and 2002/58/EC.

Overview of the Recommendations

For businesses and administrations wishing to use cloud computing services, the Opinion recommends that the data controller should first conduct a comprehensive and thorough risk analysis of the proposed cloud service. In this respect, all cloud providers offering services in the EEA should provide the cloud client with all the information necessary so that the potential cloud client can rightly assess the pros and cons of adopting the cloud service.

The document highlights the responsibilities of the cloud client as a data controller and recommends that the cloud client select a cloud provider that guarantees compliance with EU data protection legislation derived from Directives 95/46/EC and 2002/58/EC. It also stresses that the cloud client should verify whether the cloud provider can guarantee the lawfulness of any cross-border international data transfers.

 ISSN 1538-3423

Once the cloud service provider is identified, the relationship should be recorded in a contract that affords sufficient guarantees in terms of technical and organizational measures for the cloud service. The Opinion identifies a number of contractual safeguards to be included in the contract for cloud services.

Preliminary Risk Analysis

In a first series of key recommendations, the Opinion stresses that businesses and other entities wishing to use cloud computing should start their cloud computing project by conducting a comprehensive and thorough analysis of the risk associated with the project, including, in particular, an evaluation of the risk to the data that would be held in the cloud. This due diligence requires actions by the purchaser of the cloud services and cooperation from the providers of the cloud services.

Risk assessment

As a precondition for relying on cloud computing, the Article 29 Working Party recommends that data controllers perform an adequate risk assessment, including, for example, identifying the locations of the servers where the data are to be processed, and evaluating the risks and benefits of the cloud service from a data protection perspective. In particular, the analysis should address the risks related to processing data in the cloud, such as lack of control and insufficient information in view of the type of data to be processed. Special attention should also be paid to security obligations and international transfers.

Transparency

To make this risk assessment possible, the Opinion recommends that cloud providers should inform their clients about all relevant data protection aspects of their services. This includes, in particular, identifying all subcontractors contributing to the provision of the cloud service and all locations in which data may be stored or processed by the cloud provider or its subcontractors. They should also provide meaningful information about technical and organizational measures used by the cloud provider or its subcontractors.

Contractual Provisions

The second party of the Article 29 Working Party's Opinion provides guidance on the contractual arrangements that should regulate the relationship between a data controller and a cloud service provider with respect to data privacy and security. The contract should provide appropriate transparency with respect to the data handling practices. It should also ensure isolation, intervenability (the ability of data subjects to exercise their rights) and portability of the personal data. Appropriate security measures should provide the tools necessary for ensuring availability, integrity, and confidentiality. The recommendations detailed in WP 196 include the following:

Responsibility as a controller

The cloud client is subject to all the legal obligations under applicable national law implementing Directives 95/46/EC and 2002/58/EC, in particular vis-à-vis data subjects. It should select a cloud provider that guarantees compliance with these laws. The data controller should inform data subjects about the use of a cloud provider and subcontractors, and about the locations where the data may be stored or processed.

Contractual safeguards

The contract with the cloud provider, and the related contracts between the cloud provider and its subcontractors, should provide sufficient guarantees with respect to the technical security and organizational measures. In particular, the contract should detail the client's instructions to the provider including:

- Subject and time frame of the service;
- Objective and measurable service levels;
- Relevant penalties (financial or otherwise); and
- Security measures to be complied with as a function of the risks of the processing and the nature of the data.

Subcontracting safeguards

The contract should specify that subprocessors may only be commissioned with the cloud client's consent. The cloud provider should be required to sign a contract with each subcontractor reflecting the stipulations of its contract with the cloud client. The cloud service provider should inform the client of any intended changes in this regard. The cloud client should retain at all times the possibility to object to such changes or to terminate the contract. It should also ensure that it has contractual recourse in case of a breach of contract by the cloud subcontractors.

Purpose specification and limitation

The client, as a data controller, should ensure compliance with ''purpose specification'' and ''purpose limitation'' principles and ensure that no data are processed for further purposes by the provider or any subcontractors.

Data retention and disposal

The client as data controller is also responsible for ensuring that personal data are erased by the cloud provider and any subcontractors as soon as they are no longer necessary for the specific purposes. The contract should specify secure erasure mechanisms such as destruction, demagnetization, and overwriting.

Technical and organizational measures

The contract should require the use of technical and organizational measures to ensure transparency, availability, integrity, confidentiality, isolation, portability and intervenability (the ability of data subjects to exercise their rights).

Cross-border data transfers

The Opinion dedicates several pages to analyzing the conditions for the transfer of personal data out of the EEA, through the use of standard contractual clauses, adequacy findings, and Binding Corporate Rules (BCRs) for data processors. It recommends that the cloud client verify whether the cloud provider can guarantee the lawfulness of cross-border data transfers and limit the transfers to countries chosen by the client, if possible. A list of the locations in which the service may be provided should be included in the contract.

In its legal analysis of the legal framework with which cloud services must comply, the Article 29 Work-

  PVLR ISSN 1538-3423

ing Party casts significant doubts on the ability of Safe Harbor self-certification to meet the data protection requirements in effect in the EEA. The Opinion points out that ''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 . . . . The Working Party considers that companies exporting data should not merely rely on the statement of the data importer claiming that he has a Safe Harbor certification . . . . [T]he company exporting data should request evidence demonstrating that their principles are complied with . . . . It might be advisable to complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud.''

Third-Party Access to Data

Several provisions of WP 196 address the different forms of third party access to data, whether this access is by the cloud provider's own personnel or its subcontractors, or whether it is requested by third parties or by governments. The recommendations include:

Access to data

Only authorized persons should have access to the data. A confidentiality clause should be included in the contract.

Access by third parties

The contract should include an obligation for the provider to name its subcontractors—e.g., in a public digital register—and ensure access to information about any changes in order to enable the client to object to these changes or terminate the contract.

Access to data by law enforcement

The Opinion also focuses on the conditions under which foreign law enforcement agencies could have access to data stored in the cloud. It stresses that the cloud service contract should require the provider to notify the client of any legally binding request for disclosure of the personal data by a law enforcement authority, unless such disclosure is otherwise prohibited. The contract should provide that the provider will reject any non-legally binding requests for disclosure.

The WP 196 document also points out that the upcoming EU Data Protection reform should prohibit data controllers operating in the EU from disclosing personal data to a third country if so requested by a third country's judicial or administrative authority, unless this disclosure is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority.

Auditing and Monitoring

Several sections of WP 196 address the interaction between the cloud provider and its clients in connection with monitoring and auditing. It also includes a requirement for cooperation when responding to data subjects' exercise of their right of access to, and correction of, their data. The suggested provisions include:

Obligation to cooperate

The cloud provider should commit to allow the client to exercise its right to monitor processing operations, to cooperate with the client when data subjects exercise their rights to access, correct or erase their data, and (where applicable) notify the cloud client of any breach of security affecting the client's data.

Logging and auditing of processing

The cloud client should request that a log of the processing operations performed by the provider and its sub-contractors be kept. The client should be allowed to audit the log or the controller should provide a report from a third-party auditor.

Third-party data protection certifications

The WP 196 document also allows for the use of independent verification or certification by a reputable third party as a means for cloud providers to demonstrate their compliance with their obligations. Such certification would, at a minimum, indicate that data protection controls have been subject to audit or review against a recognized standard meeting the requirements set out in WP 196 by a reputable third-party organization.

Effect on U.S. Cloud Providers

Is Safe Harbor still viable?

The WP 196 Opinion raises a significant question that may constitute a barrier to the development of the cloud computing market. Its negative assessment of the viability of Safe Harbor self-certification as a way to meet the adequacy requirement of the EEA national data protection laws is likely to slow down the adoption of cloud computing in Europe, because most of the cloud providers are U.S.-based. If, as stated in the Opinion, the Safe Harbor principles may not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the United States, as may be required under national data protection laws of the EU Member States, then both the U.S. data importers and EU data exporters may be left with no certainty on how to proceed, and more questions about what will satisfy the EU regulators.

Will cloud contracts have to be updated?

The guidelines provided in the Article 29 Working Party's Opinion WP 196 go significantly beyond the current provisions of most cloud service agreements. Cloud clients have had significant difficulty obtaining information about the location of the data or the identity of the subprocessors. They also have generally been unable to control the use of subcontractors. Most contracts for cloud services do not include any significant penalties. A cloud provider's liability is usually limited to direct damages, and capped to the amount paid for the services for the few months that preceded an incident (usually two to 12 months). Most cloud contracts also do not address data retention or data disposal. The provisions that address data retention, if any, are frequently limited to granting the cloud provider the right to delete all data at the end of the relationship.

While they do not have the force of law, opinions of Article 29 Working Party have a very significant influence over the ways companies operate and the privacy choices they make. Businesses operating in the European Union should keep in mind that the data protection authority of the country or countries in which they operate are highly likely to follow the guidance set forth in a Working Party's opinion. Thus, it is important that

they operate within the guidelines and guidance provided in the opinions and other writings of the Article 29 Working Party.

Guidance from U.S. regulators?

In the United States, numerous other guidelines, guidance, and other documents have been published, from which U.S. cloud providers can derive useful practical guidelines. The Federal Trade Commission has published numerous consent decrees in connection with its enforcement actions, which provide substantial insights on what the FTC expects in terms of data privacy and data security protections. However, these documents do not focus specifically on cloud computing. The Federal Financial Institutions Examination Council has just published a document on the risks of cloud computing, titled ''Outsourced Cloud Computing,'' but the document misses the point when it characterizes cloud computing as merely another form of outsourcing.

Conclusion

It is not clear at this time what effect the Working Party's Opinion in WP 196 will have on U.S. cloud providers, and the extent to which U.S. cloud providers will adjust their operating terms in order to meet the new guidelines of the Article 29 Working Party. It is clear, however, that if U.S. cloud providers want to continue to attract EU-based clients, they will have to address the recommendations of WP 196, especially those related to cross-border data transfers, at least in connection with their sales in the European Union. Will they want or be able to keep different sets of terms for their contracts signed in the United States, when many of their clients are global companies who want to sign global deals?

  PVLR ISSN 1538-3423