Data transfers in the Cloud

Rapporteur: Emmanuelle Bartoli
Meeting date: 28th March 2014
The purpose of this document is to explore options for how contracts between Cloud providers and consumers and small firms can best ensure that the legal rules on protection of personal data are respected and that consumers and small firms can trust that they comply with their obligations vis-à-vis data subject including when their data are transferred outside the EU by their cloud providers. The Commission specifically asked to focus the discussion on contractual safeguards.

Cloud implies by essence transfers of data in general and of Personal data in particular. Indeed, one of the key characteristic of the Cloud is that data are accessible to customers anytime from anywhere and that they may be stored in different places, at the same time or at different time depending on the storage needs and on the service to be delivered.

It appears that one of the roadblock for the expansion of the Cloud computing is the fear of customers to have their data disseminated all over the world without knowing exactly where and how. Even though EU law provides for strict rules on data transfers, this fear remains an obstacle to take-up and growth of Cloud opportunities.

The overall discussions that will be taking place during our Subgroup meeting on 28th March 2014 should be driven by the need to bring more confidence in the Cloud computing.

**Some quotes to have in mind**

“Cloud is about how you do computing, not where you do computing.” - Paul Maritz, VMware CEO

“Cloud computing is empowering, as anyone in any part of world with Internet connection and a credit card can run and manage applications in the state of the art global data centers; companies leveraging cloud will be able to innovate cheaper and faster.” - Jamal Mazhar, Founder and CEO – Kaavo

“If European cloud customers cannot trust the United States government, then maybe they won’t trust US cloud providers either.” - Neelie Kroes, European Commissioner for Digital Affairs, in an interview on the NSA fallout revelations
1. Referring to data transfers in the contract

**QUESTIONS**

1. Should the contract contain clauses governing transfers outside the EU take place?
2. How precise should those clauses be, beyond the legal obligations?
3. Should the clauses cover any data, or specifically refer to personal data?

The contract should first of all make it clear that EU data protection law applies with respect to the personal data being transferred or otherwise processed.

EU data protection law requires compliance with a number of key principles. These data protection principles must continue to be respected even when the personal data is transferred or otherwise processed outside of the EU.

Where the contract provides a description of the transfers, this ensures that there is clear information with respect to how and where data is transferred and processed.

The scope of the transfers under the responsibility of the cloud provider and the ones under the responsibility of its client can also be clarified.

2. Legal basis for the transfer

**QUESTIONS**

1. Shall the contract clarify the legal ground used to legitimize transfers?
2. How should onward transfers be addressed / in particular should they be covered by specific clauses or under the general transfer clause?

International data transfers out of the EU are generally legally permitted only where one of the conditions below is fulfilled:

1. Adequacy (Safe harbor is a partial adequacy)
2. BCR
3. Model clauses
4. Ad hoc contracts (+ authorization in accordance with national laws implementing 95/46)
5. Consent
6. Derogations
Under national legislation implementing Directive 95/46/EC, national data protection authorities may have requirements in relation to their authorization of transfers on the basis of adequate safeguards.

The objective of this exercise is to ensure that mechanisms for ensuring an adequate level of personal data protection when data is transferred outside the EU are appropriate to how cloud providers and their customers organize data transfers. We shall discuss the pros and cons of each mean.

2.1 Consent

QUESTION
1. Do some cloud providers invoke the consent of data subject to legitimize international transfers, in the context of contracts with consumers or small firms?
2. Do you see transfers situation where the transfer necessarily requires the consent of the data subject?
3. Should the cloud provider or the customer obtain the consent? If the customer is in charge of the consent, should the cloud provider provide some tools to assist with obtaining such consent?

Obtaining the consent of each data subject in the context of Cloud computing appears to be a challenge to say the least.

How to reasonably believe that in the Cloud environment especially where….

- … the numbers of data subjects is high and,
- the purposes for which the data may be processed are not always known from the cloud provider and,
- The locations from where the data may be processed evolve constantly…

…consider that consent can be obtained?

2.2 Derogations found in article 26 of the EU Directive

Given that the Working Party 29 has considered in a working paper relating to data transfers\(^1\) that exemption should only apply to non-massive, non-recurrent and non-structural transfers, it appears

almost impossible to rely on exemptions in the Cloud computing environment. This is also the opinion put forward by the Working Party 29 in its working paper on Cloud computing\(^2\).

2.3 Transfer to an adequate country

**QUESTION**

Should transfers to adequate countries be referred to in cloud contracts separately from transfers under other legal grounds?

The list of countries being considered as providing an adequate level of protection by the EU Commission is quite restricted. In addition, the listed countries are not necessarily the countries where the Cloud activities and/or maintenance activities are more developed.

Given the limited number of countries listed as being adequate, the situations where it will be possible to rely on adequacy will be limited.

Hopes are permitted regarding an increase of the number of countries that will be qualified as adequate by the data EU Commission as a result of the provisions of the EU Draft Regulation which calls for a simplification in the adoption of adequacy decisions.

2.4 Adequate safeguards provided by controller

**QUESTIONS**

1. Which model is best suited to the need of consumers and small firms: ad hoc safeguards or EU model clauses / standard clauses?
2. In case of ad hoc safeguards used by data controllers, what could be the appropriate procedure to ensure that those safeguards are sufficiently protecting the data subjects and the consumer and small firms?
3. Would the current set of clauses adopted by the Commission need to be revised – specifically for the cloud, or generally speaking?
4. In particular, should the work currently ongoing around processor to processor clauses be endorsed in a model clause decision from the Commission (see explanations below)?
5. Should the standard clauses elaborated by DPAs in 14 MSes be streamlined into some EU wide standard clauses?

The current EU Directive enables transfer to third countries where controllers are able to demonstrate that they have provided adequate level of protection to the data transferred (Article 26.2 of the EU Directive 95/46).

As part of this working group, the Commission indicated willingness to consider if necessary a review of the standard contractual clauses, if some issues are identified as regards the existing clauses.

### 2.4.1 Ad hoc mean of processing

Such provisions may be quite attractive as it seems to introduce flexibility in the system and leaves it up to the data controller to provide the level of protection. However, this is just an illusion, especially in the Cloud environment.

**Why?**

(i) It relies on Data controller to ensure the adequacy of the transfer. In the context of Cloud even more than in the classical outsourcing model, leaving to the Data controller (i.e. Cloud provider the responsibility) the responsibility to frame the transfer of data is illusory as in the end we know that the Cloud provider is the one deciding which tool should be used and how.

(ii) Leaving to the data controller the possibility to determine what is providing adequate level of protection creates legal uncertainty as there is no possibility for the parties to anticipate what will and what will not be adequate.

### 2.4.2 Standard EU Model Clauses

It results from the above that the EU Model clauses as adopted by the EU could be the privileged legal instrument to frame data transfers from the EU to outside of the EU.

They create legal certainty and given that they are standards they should not require huge efforts *per se* to be agreed and signed amongst the parties.

The current EU Model Clauses that are classically used in outsourcing and/or Cloud processing are the ones resulting from the Decision adopted by the European Commission dated 5 February 2010 (“EU Model Clauses 2010”)\(^3\). These clauses apply where the 2 criteria are fulfilled:

(i) a transfer from a data controller to another entity

(ii) the importing entity should be located out of the EU.

---

In practice, this means that the transfers made by a data processor located in the EU are not covered by the EU Model Clauses 2010. This is quite annoying as, in practice, this situation is the most usual one.

See chart below:

Recital 23 of the EU Decision adopting the EU Model Clauses 2010 provides that:

“Since this Decision applies only to subcontracting by a data processor established in a third country of his processing services to a sub processor established in a third country, it should not apply to the situation by which a processor established in the European Union and performing the processing of personal data on behalf of a controller established in the European Union subcontracts his processing operations to a sub processor established in a third country.”

As a result, the EU Model Clauses 2010 cannot be used to frame the transfer made by the Cloud provider in the EU. These clauses need to be signed between the data controller and the data importer(s) located outside the EU directly.
In practice, this is clearly inappropriate and not feasible in the Cloud environment. Indeed, if one intends to frame the transfers with the EU Model Clauses 2010 this means that each Customer needs to sign with the different entities (and/or service providers) located out of the EU. One will understand immediately the number of contracts to be signed and the paper work such an approach would imply. The example that follows will illustrate particularly this statement:

Take a Cloud provider located in the EU and which has 4 data centers located in different countries outside the EU. This Cloud provider has 2500 customers located in the EU. If its Customers acting as Data controllers intends to frame the transfers with the EU Model Clauses 2010, this means that in total 10 000 EU Model Clauses will have to be signed (2500 customers X 4 data centers. One can really question the legal interest of such an exercises as well as the added value.

In addition, it is important to note that in many situations, Customers are reluctant to enter into contractual relationship with a legal entity they have never contracted with before. In order to address this last criticism, the Working Party 29 (WP29) has adopted a FAQ\(^4\) which proposes another solution, having similar legal effects to those of the first solution but with different modalities. It consists of including in the service provider agreement a clear mandate to the Cloud provider to sign the EU Model Clauses 2010 with the non-EEA-based entity of the Cloud provider (and/or the sub processor) in the name and on behalf of the Customer. The latter remains the data exporter and the entity of the Cloud provider (and/or the sub processor) is the data importer. It is also stated that the controller should also agree in advance to the content of Appendices 1 and 2 of the EU Model Clauses 2010. Here again in practice this is not possible in the context of the Cloud environment and this would definitely not solve the paperwork described above – it would just transfer this workload on the Cloud provider.

2.4.3 Call for an alternative solution

It results from the previous section, that the current EU Model Clauses 2010 which aim at covering transfers from Data Controllers to Data Processors have some limitation in the context of Cloud computing.

(i) Why?
The main reason which explains the difficulty described above is the fact that the responsibility to frame the transfer is on the sole side of the consumer or small firm when acting as Data Controller.

(ii) How?
The proposed approach should be to have clauses which would enable data processor to provide itself the guarantee for the data transferred. This approach exists already in Spain and should definitely be pushed at EU Level.

Indeed, in December 2012, the Spanish Data Protection Authority (SPDA) published a new set of Model Clauses prepared purely for use by service providers that subcontract to companies located in countries outside the EEA.

These clauses are based on the EU Model Clauses 2010 and allow data transfer between a data processor which is then considered as a data exporter established in Spain to a sub processor (data importer) based out of the EU.

In practice this means that Spanish Cloud providers acting as data processors can enter into Model Clauses directly with their sub processors and initiate the prior authorization process themselves with the SPDA to request approval of an international transfer of their client’s personal data for processing by their subcontractors located outside the EU.

These new Model Clauses should facilitate data processing within a supply chain by allowing outsource service providers to engage subcontractors outside the EEA, serve as evidence to customers of their data protection compliance and ultimately market their services in a more competitive fashion. The Spanish DPA has clearly responded to the demands of the outsourcing sector by providing a more flexible method of covering processor-to-sub processor data exports and helping to eliminate some of the regulatory barriers that place EU processors at a competitive disadvantage with their non-EEA competitors.

Such approach should be promoted and the industry should call the EU Commission to work on the adoption of a Decision that would enable Cloud providers to use this kind of clauses.
2.5 Binding Corporate Rules

**QUESTION**

How should the BCRs be reflected in the contracts between cloud providers and consumers and small firms?

The Binding Corporate Rules (BCR) are equivalent to a Group Data protection policy that would be officially validated by all EU data protection authorities as providing an adequate level of protection for transfers made within a group of entities bound to respect the said group policy. Therefore, BCR provide a global approach and leave the responsibility to frame the transfers to the Cloud provider. In the context of the Cloud, the newly recognized BCR for processors\(^5\) are more than welcomed as they enable an entity acting as a data processor to bear the burden to frame the transfer of data.

BCR are known to be the most comprehensive and secured approach to frame international transfers as they imply a commitment from a group of entities to respect the same principles and to implement the measures and procedures to ensure the effective respect of these principles.

However, BCR cover transfers only where the transfers are made within a group of entities and do not cover transfers made to third parties involved in the processing of the services that a Cloud provider can deliver. Or, Cloud environment prove to be complex and the number of stakeholders involved in the processing tend to be much more important than what it is in the usual outsourcing offers. Therefore, even though the BCR clearly provide an improvement on the guarantees brought to the data transferred in the Cloud environment one should not forget that this will not cover the transfers out of the EU made to third parties located out of the EU.

2.6 Safe Harbor

**QUESTIONS**

1. How should adherence with safe harbor be reflected in cloud contracts with Consumer and small firms?
2. Should the possibility of onward transfers under safe harbor be addressed in the contract, and if so, how?

In 2000, the US Department of Commerce and the European Commission agreed on the Safe Harbor scheme which sets out a framework of data protection standards which allow the free flow of personal data from EEA data controllers to the US organisations which have joined the scheme.

---

US companies that adhere to the Safe Harbor data protection standards, principles and procedures will be deemed to provide an adequate level of protection which satisfies the EU Directive 95/46 requirements.

This approach is very flexible and at first glance would enable to have sufficient guarantees to the transfers made from the EU to companies located in the US and declaring their adhesion to the US Safe Harbor.

When reviewing the Safe Harbor Agreement and assessing its effectiveness, the EU Commission has pointed the need for more cooperation between EU and US authorities in order to ensure more efficient respect of the Safe Harbor principles.

The WP29 paper on Cloud computing calls for paying particular attention to the guarantees brought by companies claiming they are Safe Harbor certified. This would help customers assessing whether such claim is founded and whether the company effectively applies the principles.

VI. Third country authorities request of access

**QUESTIONS**
1. Shall standard clauses on Cloud computing address public authorities request of access?
2. What kind of obligations could apply to the cloud provider, beyond transparency?
3. How could the infringement to fundamental rights be minimized in contractual obligations?

The NSA revelations have put on the forefront the question how public authorities can request access to data stored by Cloud providers.

Most Customers request Cloud providers to (i) inform them in case they receive such request and (ii) resist where possible to such request.

In certain situations, under the Patriot Act for instance, Cloud providers are not allowed to communicate to Customers the fact that a request has been received from the US Authorities. Therefore, there is a need of pedagogy to explain to Customers that they can't be informed in all circumstances of such request.
It would be in the interest of both parties to make sure that Cloud providers have internal policies explaining how to handle such request. A reference to such policy in the standard clauses for Cloud would provide more security and guidance to Customers.