Security and privacy regulatory challenges in the Cloud

The 2012 European Cloud Computing
Making the Transition from Cloud-Friendly to Cloud-Active
Brussels, 21st March 2012

Giovanni Buttarelli
Assistant European Data Protection Supervisor

Speaking notes

Ladies and gentlemen,

Allow me to begin by thanking the organisers of this conference for their invitation. It gives me great pleasure to be able to contribute to your discussions.

At the beginning of March the EDPS issued an Opinion on the new proposed European data protection framework that tackled, among others, issues associated to cloud computing. Still, we believe that this topic deserves specific attention and I would like to announce to you that the EDPS will issue an Opinion on the impact of the new proposed Regulation on Cloud computing in the next few months.

For this presentation, I am not going to refer in detail to all the challenges raised by the cloud1 but I will focus my speech on how the draft Regulation would tackle the following issues: (i) the notions of controller and processor, (ii) applicable law, (iii) accountability, and (iv) coordinated supervision and enforcement.

Improving the allocation of roles and responsibilities (the notions of controller and processor)

Under the current Directive, the controller is the one who determines the 'purposes and means' of the processing2. The draft Regulation adds that the controller is also the one who determines the 'conditions' of the processing. However, the distinction between data controllers and data processors has become increasingly complex and blurry, especially in the cloud environment. While in most cases cloud users should be considered to be the controllers and cloud providers

---

1 Notwithstanding this, in the speaking notes that will be distributed you will find a list of the main challenges along with some reflections on how are tackled by the current Data Protection legislation and also by the draft proposal for a data protection Regulation that has been made by the European Commission.  
2 The criteria for distinguishing whether an organisation is a controller or a processor were clarified by the Article 29 Working Party in its Opinion 1/2010 on the concepts of ’controller’ and ’processor’, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.
should be considered as processors, the extent to which cloud service providers are solely acting as processors remains often uncertain. This is due in particular to the fact that cloud service providers often not only determine the means of the processing, but also offer features which contribute to some extent to determining the conditions and the purpose of the processing.

There are therefore a number of situations where cloud service providers will be co-controllers of the processing together with the cloud client. Such cases are tackled in the draft Regulation which sets forth a regime of joint liability of controllers (Article 24).

One area that will require further reflection is the issue of defining the specific obligations and liability that should be imposed on cloud providers acting as processors. The draft Regulation foresees that a number of obligations should be imposed by contract upon the processor, including on their need to help the fulfilment of controller's obligation to ensure the exercise of data subjects' rights (Article 26). However, because of the significant power a cloud provider has to impose its terms and conditions upon cloud clients, leaving this issue to contractual arrangements between parties may not be sufficient. There may be a need to legislate further or at least to reflect on what other specific measures would be needed to address the specific obligations and the liability upon the cloud providers. The release by the Commission of its Cloud Strategy due, as announced this morning, for July, may provide helpful steps in this direction.

**Clarifying applicable law**

Within the EU, the difficulty of identifying what is the applicable law governing the processing activities of a controller or a processor having one or several establishments in the EU is being tackled in the draft Regulation in several ways.

- First, the choice of a Regulation as the legislative instrument for the new data protection framework will contribute to having one single law applicable throughout Europe. The draft Regulation sets forth a number of obligations addressed both to controllers and to processors established in the EU. This will help provide greater consistency in Europe, although specificities will remain possible at national level in a number of areas for which national law has specific competence (e.g. employment law), derogates from or builds upon the draft Regulation.
- Second, the draft Regulation introduces the notion of 'main establishment' in the EU in order to identify the competent supervisory authority in respect of controllers and processors who have several establishments in the EU (Article 4(13)). However, it does not solve the issue of the extent to which specific data protection national laws applying to the main establishment would have to be complied with in other undertakings located in the EU.

As concerns controllers located outside the EU, the draft Regulation makes it clear that they would fall under the scope of EU data protection law if they engage into the following processing activities:

- the offering of goods or services to data subjects in the European Union; or
- the monitoring of the behaviour of data subjects residing in the European Union. Such monitoring activities would notably include profiling activities on the internet, which are aimed at taking decisions about them or for analysing or predicting their personal preferences, behaviours and attitudes (recital 21).

For instance, if a Chinese controller is offering services in the cloud to UK customers and has all its web pages in English and it offers a customer support phone number for UK customers, one should conclude that the Chinese company is a controller offering services to UK customers and that it falls under the scope of the EU data protection law.
As concerns processors located outside the EU, although they would not fall within EU jurisdiction as such, they would nevertheless in practice have to adapt their practices to meet some of the European data protection law requirements if they want to engage into business with EU controllers (in particular the respect of obligations imposed on processors and in the frame of third country transfers mechanisms).

Finally, I also want to stress that an additional level of complexity in the cloud is the possibility for controllers and processors to be subject to cumulative jurisdictions.

**Making actors in the cloud more accountable (the principle of accountability)**

By introducing the principle of accountability, the draft Regulation shifts from a regime of bureaucratic notifications of processing operations to a regime whereby the controller must ensure and demonstrate at all times that he complies with all the obligations set forth in the draft Regulation. There are a number of fine tuning measures that still need to be adopted to specify in more details how accountability will be achieved in practice, but in the whole this is a significant step forward in the way Europe is approaching the notion of compliance.

Furthermore, the draft Regulation introduces a dose of accountability also in respect of processors who have establishments in the EU, such as by requiring them to maintain documentation of their processing operations, to carry out data protection impact assessments of risky processing activities or by requiring them to ensure an adequate level of protection of data they transfer outside the EU. Many cloud service providers who have establishments in the EU will therefore be subject to these types of measures, which shall contribute to increasing the level of data protection of the processing activities they carry out in the EU.

**Improving coordination mechanisms at EU and global levels**

One of the challenges in the cloud, directly linked with the issue of applicable law, is the difficulty to exercise any form of supervision in the cloud. The multiplicity of actors and the diversity of locations where data processing operations take place in the cloud call for the development of mechanisms facilitating the coordinated supervision of these activities. The consistency regime foreseen in the draft Regulation is, in this view, particularly welcome. It should help provide a uniform approach of supervisory authorities within the EU on topics which are transnational by nature, such as the cloud. Furthermore, the enforcement powers of supervisory authorities have been increased in the draft Regulation by laying down the possibility to apply financial sanctions, and the range of such sanctions.

However the above mentioned consistency mechanism only solves the problems at EU Level and the cloud has to be considered in a global context. Therefore there is also a need to invest in global solutions and to enable a greater level of coordination at international level. This was particularly emphasised by the speakers this morning. At technological level solutions and standards are currently being developed to encourage interconnection and interoperability.

Finally let me conclude by saying that the essential aspect is not the name of the instrument that we use, the essential aspect is that data protection is adequately protected and how legal concepts can be implemented. We must be innovative and we do not have to restraint ourselves to a single model. The draft Regulation is a first step in that direction. Other measures and complementary actions will also have to be explored in order to appropriately tackle the issues that are specific to the cloud.

Thank you for your attention
ANNEX I. SIMPLIFYING INSTRUMENTS FOR INTERNATIONAL TRANSFERS

The limits of current instruments for international transfers

One of the conditions in EU law for a data processing operation happening in the cloud is the existence of an adequate level of protection in the country or countries outside the EU involved or, in the absence of a positive decision concerning the adequacy of the level of protection of the countries outside the EU involved, that certain safeguards may serve to permit the transfers of data and the processing activities. This is where measures come in such as: **Standard Contractual Clauses, Binding Corporate Rules or Safe Harbour.**

- **Standard Contractual Clauses.** The European Commission has adopted standard clauses that have been analysed and found adequate. This brings some advantages for the controllers and the data protection authorities in charge of the supervision in terms of legal certainty and binding force. The main advantage for the controllers is that, in principle, the transfer (and therefore the data processing activity) does not need prior authorisation and a notification to the data protection authority will suffice. Given the dynamicity of the cloud, the possibility of operating without prior authorisation brings an enormous benefit for controllers in the cloud, however the requirement to sign a contract and notify data protection authorities for all the parties involved (and in cloud computing this can be a lot) reduces its applicability.

- **Binding Corporate Rules.** The adoption of BCRs is intended to make it easier to transfer data within groups of companies when some of the addressees are established outside the European Union. As you know the binding corporate rules are not explicitly foreseen in our current Directive but have developed as a matter of practice, with the support of Article 29 Working Party which gathers data protection authorities from all Member States. While the goal is first and foremost to provide an adequate level of protection for such transferred data, BCRs provide a harmonised solution for all intra-group exchanges in cases where there is a connection with the European Union. Businesses adopt them voluntarily and then ensure that there are adequate safeguards for transfers of data between companies that are part of the same corporate group. Notwithstanding this, the process usually becomes very lengthy since, in the absence of some common rules, all the 27 DPAs have to approve the code of conduct.

- **Safe Harbor.** It is a streamlined process for US companies to comply with the EU Directive 95/46/EC on the protection of personal data intended for organizations within the EU or US that store customer data, the Safe Harbor Principles are designed to prevent accidental information disclosure or loss. US companies can opt into the program as long as they adhere to the 7 principles outlined in the Directive. However, I must say that it is legitimate to discuss if they provide for an adequate level of protection, since they contain fewer obligations for the controller and allow the contractual waiver of certain rights.

---

3 The adequacy level that is assessed in the first instance by the European Commission but also, where appropriate, by the data protection Authority of a Member State.

4 Adequacy decisions adopted by the European Commission are limited in number. Today they relate to a dozen or so countries, including Argentina, Canada, Israel, Switzerland, Jersey, Guernsey and the Isle of Man; as far as the United States is concerned, the Commission decides on data transfers to companies that have opted into the Safe Harbor programme. The full list of decisions on the adequacy of data protection can be consulted on the website of the Directorate-General for Justice of the European Commission.

5 See Annex for further details.

6 The Data Protection Authority will confine to verify that the clauses set out in the Commission’s decision have not been altered and that there is no evident risk of their terms being breached in the country of destination.

7 Also it is worth mention Cross-Border Privacy Rules. It is a parallel model with a lot of similarities to BCRs being discussed alongside the European system in the Asia-Pacific Economic Cooperation forum.

8 Binding means legally binding. It means that an agreement has been consciously made, and that the parties bound by the rules knowingly understand that they agree to make certain actions either required or prohibited. Therefore they could be brought before a court.
Use of consistent transfer mechanisms that are fit for the cloud

However, for different reasons the mechanisms envisioned, have proven to be, in many cases, burdensome or ineffective or have lacked of the necessary flexibility.

In this context, the speech\(^9\) of Commissioner Vivianne Reading mentions that binding corporate rules should be regarded as an instrument open to innovation, open to international interoperability, open to improve data protection on a global scale and open to go beyond the geographical borders of Europe.

Indeed, binding corporate rules can become a cornerstone to enable the necessary international cooperation to foster the adoption of cloud services while ensuring the needed trust in the protection of fundamental rights such as the right to data protection. In the particular case of BCRs, the following aspects are important to enable their application to cloud computing:

- **Explicit recognition of BCRs** in European data protection law is ensured in the draft Regulation.
- **Establishment of a simplified procedure.** The draft Regulation foresees that it should be possible for BCRs to be validated on the strength of the approval of only one data-protection authority and have the same binding force throughout the European Union. It is still unclear if this simplification will be enough but it is clearly a step in the good direction.
- **Extend the application of BCRs beyond "intra-group".** BCRs should apply not only intra-group but also to processors and “joint-controllers”. These possibilities to extend the scope of application of BCRs are particularly important as they take better account of the cloud environment.

---

\(^9\) SPEECH/11/817 Date: 29/11/2011 Binding Corporate Rules: unleashing the potential of the digital single market and cloud computing.
ANNEX II. HOW THE MAIN PRIVACY AND SECURITY CHALLENGES RAISED BY CLOUD COMPUTING ARE TACKLED IN DIRECTIVE 95/46/EC IN COMPARISON TO THE DRAFT REGULATION

<table>
<thead>
<tr>
<th>Challenges of the Cloud</th>
<th>How they are addressed in Directive 95/46/EC</th>
<th>How they are addressed in the draft Data Protection Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harmonisation inside the European Union</td>
<td>- Directive 95/46 has been transposed into national legislation with some divergences and inconsistencies.</td>
<td>- The new framework proposed is a Regulation that will be directly applicable. Also it incorporates consistency mechanisms (Articles 57,58,59,60,61,62,63)</td>
</tr>
<tr>
<td>Role of the actors (Controller / Processor)</td>
<td>- Controller determines the 'purposes and means' of the processing (Article 2(d)). + Opinion 1/2010 of the Article 29WP on the concepts of 'controller' and 'processor'</td>
<td>- Adds one criterion to distinguish the controller as the one who determines the 'purposes, conditions and means' of the processing (Article 4(5)). - Extends part of the obligations of the controller to the processor. - Need for an arrangement between joint controllers (Article 24). - Detailed processors and sub-processors obligations (Article 26).</td>
</tr>
<tr>
<td>Applicable Law</td>
<td>- <strong>Intra-EU</strong>: sets forth the criteria of what is the national applicable law; if establishments in several Member States, the controller must ensure that each of these establishments complies with the obligations laid down by the national law applicable (Article 4(1)(a)). + Opinion 8/2010 of the Article 29WP on applicable law</td>
<td>- <strong>Intra-EU</strong>: one single data protection law applicable within the EU (effect of the Regulation), unless exceptions apply. - Draft Regulation clarifies that it applies to the processing of data by controllers as well as processors who have an establishment in the EU (Article 3(1)). - In case of multiple establishments, the criteria for determining the 'main establishment' of the controller and of the processor are set forth in recital 27 and Article 4(13).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Extra-EU</strong>: the processing of a controller established outside the EU may fall under EU law if the controller uses equipment situated on the territory of the said Member State (Article 4(1)(c), and such equipment is not used only for purposes of transit through the territory of the EU. However, notions of 'use</td>
<td>- <strong>Extra-EU</strong>: applicability of EU law to a controller established outside the EU if the processing is related to (i) the offering of goods or services to data subjects in the EU, or (ii) the monitoring of their behaviour' (Article 3(2)). - Designation of a representative (Article 25), but exceptions.</td>
</tr>
<tr>
<td>Category</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| Accountability                 | - General responsibilities of the controller, but no clear 'accountability' provision as such (Article 6(2) and Article 17)  
- + Opinion 3/2010 of the Article 29WP on the principle of 'accountability'  
- Principle of accountability is clearly set forth in Article 22, which requires the controller(s) and processor(s) to implement a number of policies and measures.  
- Controllers and processors are under an obligation to maintain documentation about the processing operations (Article 28).                                                                                          |
- + Practice of BCRs developed by Article 29WP  
- Explicit recognition of BCRs' mechanism (Article 43).  
- BCR mechanism is available both to controllers and to processors.  
- Article 45 foresees further international cooperation.                                                                                                                                                           |
| Transparency                   | - Minimum information to be provided by the controller to data subjects (Articles 10 and 11)  
- Adds, amongst others, that data subjects must be informed about retention periods and about transfers to third countries. (Article 14).                                                                                                                                   |
| Rights of the Data Subjects    | - Right of access, right to object, rectification and erasure (Articles 12, 14 and 15).  
- Creates a right to data portability in digital environment (Article 18).  
- Strengthens the right to erasure to a right to be forgotten in the digital environment (Article 17).  
- The controller must establish procedures to ensure the effective exercise of data subjects' rights (Article 12).                                                                                                                                                                        |
| PIA                            | - Not expressly mentioned/ general security obligations (Article 17).  
- Need for PIA when processing presents specific risks to rights and freedoms of individuals by virtue of their nature, their scope or their purposes. This includes in particular specific types of processing (e.g. profiling) or processing of certain data (e.g. sex life, health, etc) on a large scale (Article 33).  
- PIA must be conducted either by the controller or the processor.                                                                                                                                                                                                       |
| Privacy by design and by default | - Not expressly mentioned/general security obligations (Article 17).  
- A dedicated Article on data protection by design and by default (Article 23).                                                                                                                                                                                                 |
<table>
<thead>
<tr>
<th>Security</th>
<th>Confidentiality and security rules. However, national security obligations diverge (are more or less detailed) according to national law (Articles 16 and 17).</th>
<th>Rules on data security, which may be subject to further harmonisation through implementing acts (Article 30). A general data security breach reporting obligation is set forth (Articles 31 and 32).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standardisation</td>
<td>Codes of conducts (Article 27)</td>
<td>Codes of conduct (Article 38) and certification such as data protection seals and marks (Article 39).</td>
</tr>
<tr>
<td>Access for Law Enforcement Purposes</td>
<td>Exemptions and restrictions are possible (Article 13).</td>
<td>Exemptions and restrictions are possible (Article 21). Access by law enforcement outside the EU must respect the obligations on transfers to third countries (recital 90).</td>
</tr>
</tbody>
</table>