Deliverable 3.5.

Guidelines on how to protect personal data in cloud service contracts

www.ictlegalconsulting.com

www.cloudwatchhub.eu

Table of contents

1. Introduction and objectives

The array of cloud computing technologies and services is evolving at a fast pace and new ways of delivering IT services have emerged on the market, also driven by the explosion of the power and capability of many mobile devices. According to Gartner, enterprises should, for example, start thinking of "hybrid" cloud computing solutions and procure services accordingly, in order to match personal clouds and external private cloud services. [1]

The legal models accompanying these developments are evolving too, though not at the same pace.

Increasing attention is paid by cloud service clients (hereinafter also "CSCs") to cloud computing contracts, which are nonetheless still framed in standard forms by cloud service providers (hereinafter also "CSPs").

The contractual clauses to which cloud clients usually pay the most attention pertain to:

- exclusion or limitation of liability and remedies, particularly regarding data integrity and disaster recovery;
- service levels, including availability;
- security and privacy, particularly regulatory issues under the European Union Data Protection Directive;[2]
- lock-in and exit, including duration, termination rights, and return of data upon exit from the contract;
- the ability of the provider to unilaterally change for service features. [3]

The objective of this document is to provide some basic guidelines to cloud clients when entering a cloud computing contract. A series of recurrent contractual issues has been identified and addressed in a short and comprehensive way from the data protection law standpoint. References to other checklists and standards tackling issues critical for cloud services are also provided when relevant.

These guidelines are not meant to be exhaustive and cannot replace the legal advice provided by expert lawyers when negotiating cloud service contracts.

The guidelines have been drafted by **ICT Legal Consulting** for informative purposes only. The guidelines will be available in the "*Legal Tips*" section of **www.cloudwatchhub.eu**. They constitute the Deliverable 3.5. under the contract with the European Commission for the European project entitled CloudWATCH, reference number 610994.

[1] Gartner's Top 10 Strategic Technology Trends for 2014, http://www.forbes.com/sites/peterhigh/2013/10/14/gartner-top-10-strategic-technology-trends-for-2014/.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050 (hereinafter "Directive 95/46/EC").

[3] These issues have been found by a research into negotiated contracts performed by W. Kuan Hon, Christopher Millard & Ian Walden in *Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now*, 16 STAN. TECH. L. REV. 81 (2012) - http://stlr.stanford.edu/pdf/cloudcontracts.pdf.

2. Pre-contractual phase

a. Risks and opportunities for the Cloud service client

«Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction»[4]

Users are attracted to cloud services due to the features inherent to the cloud model, such as the possibility to access a broad network, the ability to pool and optimize resources, access services with elasticity and scalability, all while reducing the costs and, to some extent, the regulatory risks.

The outsourcing of computational, storage and platform services to cloud service providers, however, does not come without risks, especially for the protection of personal data processed in the cloud.

The European DPAs have organized the major risks for privacy and protection of personal data in the cloud into two categories:[5]

- Lack of control over personal data
- Lack of information on the processing of personal data

Pondering the trade-off between the expected advantages of outsourcing to cloud providers and the risks arising for personal data in the cloud is a preliminary step that every organization has to take before purchasing cloud services. [6]

b. Deciding whether or not to outsource cloud services

In view of contracting cloud services with big providers, customers are advised to perform both an internal and external due diligence check.

Legal tips and recommendations:

- ***As for the internal due diligence, clients should:***

[4] National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, Page 3. Available at the following website: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[5] Article 29 Working Party, "*Opinion 05/2012 on Cloud Computing*", Adopted on July 1st 2012, pp. 5-6. Available at the following website: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[6] For a complete overview of the risks posed by cloud computing read ENISA's paper on Cloud Security Risk Assessment, available here https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

- *Define their privacy, security and compliance requirements;*
- *Identify what data, processes or services they want to move to the cloud;*
- *Analyze the risks of outsourcing services to the cloud;*
- *Identify what security controls are needed to protect their employee data once transferred to the cloud;*
- *Define responsibilities and tasks for security control implementation;*

- *As for the external due diligence, clients should:*
  - *Assess whether the provider meets their privacy and data protection requirements using the **PLAs**;*
  - *Check whether the provider holds any certification or attestation released by an independent third party;*
  - *Consider whether the terms of service can be amended, how and by whom;*
  - *Understand whether and how to monitor the security controls implemented by the provider.*

3. Entering a cloud service contract: major issues

The following represent some recurrent issues identified when negotiating a contract for the provision of cloud services, based on ICT Legal Consulting's direct and indirect experience.

a. Jurisdiction & Applicable law

Cloud service contracts often contain clauses whereby the competent jurisdiction and the applicable law are set by the agreement between the parties involved.

A distinction has to be made between the two concepts.

Finding the competent jurisdiction means allocating the enforcement of the contract to a certain, competent judge, whereas finding the applicable law means finding the set of substantive rules applicable to a given contract. A possible consequence of this distinction may be that a judge of Member State "A" is called to enforce a cloud computing contract, or a part thereof,[7] on the basis of the law of Member State "B".

From a purely contractual standpoint, the parties autonomously decide in what jurisdiction they want the contract to be enforced. Theoretically, the possibility to mutually set the competent jurisdiction is recognized by the principle of contractual liberty; in practice, the cloud service provider is the entity that decides the competent *forum*, whereas the client often only has the opportunity "to take it or leave it".

Regarding the applicable privacy law, Data Protection Directive 95/46/EC applies in every case where personal data are being processed as a result of the use of cloud computing services. Another piece of

[7] A clear example of the potentially complex interplay between jurisdiction and applicable law is given by Article 17.3 of Directive 95/46/EC. It stipulates that the law regulating the security measures of a data processing agreement is that of the Member State in which the processor is established. Consider that a cloud computing contract sets the jurisdiction in the Member State in which the controller is established (Member State "A"). In this case the judge of Member State A would apply the law of the processor's Member State ("B") when enforcing the contractual provisions regulating the security measures agreed in the contract.

relevant legislation is the e-privacy Directive 2002/58/EC, whose application is triggered by the provision of publicly available electronic communications services in public communications networks (telecom operators) by means of a cloud solution. When the cloud computing provider is also a provider of publicly available electronic communications services in public communications networks, this law applies.

The criteria for deciding which law is applicable to the processing of personal data performed by a cloud computing network are provided for in Article 4 of Directive 95/46/EC, which distinguishes between controllers established in the EEA and controllers located outside the EEA.

When a data controller[8] is established in the EEA, the applicable law is the one of the Member State where it is established; when different establishments of the same controller are present, the applicable law is that of each of the Member States in which the processing of personal data occurs.

For controllers established in a third country, that nonetheless uses automated or non-automated equipment located in the territory of a Member State, the latter's law applies, except when the equipment is used only for purposes of transit. This means that if a cloud client is established outside the EEA but procures services from a cloud provider located in the EEA, the provider exports the data protection legislation to the client.

Legal tips and recommendations:

- ***Contractual arrangements regarding the jurisdiction and the applicable law are found in the Cloud Service Agreement;***
- ***In the EU, the applicable privacy law is the one of the Member State where the data controller is located, which means the law of the State where the cloud client resides, as explained in the next paragraph.***

b. Privacy Roles

A correct understanding of the roles in the processing of personal data performed by means of cloud computing technologies is functional to the correct allocation of legal obligations and responsibilities between the parties of a cloud computing contract.

According to the standard allocation of responsibilities,[9] the controllership of personal data processed in the cloud belongs to the client, whereas the cloud service provider is usually the data processor. [10]

[8] In the standard allocation of roles, the data controller is usually the client of a cloud service provider. Further details on the allocation of roles are provided in paragraph 3.b of these guidelines.

[9] This model is taken as a reference by the European DPAs in "*Opinion 05/2012 on Cloud Computing*", Adopted on July 1st 2012, p.7.

[10] According to article 2 (d) and (e) of the Directive 95/46/EC, the 'controller' is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data, whereas the 'processor' is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

This means that, whatever the imbalance in size between the client and the cloud service provider, the former is a data controller, and as such must accept responsibility for abiding by data protection legislation and is responsible and subject to all the legal duties that are addressed in Directive 95/46/EC. A certain degree of autonomy can be left to the cloud provider in the choice of the methods and the technical or organisational measures to be used to achieve the purposes of the controller.

Further complexity to this scheme is often added by data processors who avail themselves of subcontractors/subprocessors in the provision of cloud services.

Legal tips and recommendations:

- ***Clearly allocate the data protection roles between the parties;***
- ***Choose a cloud service provider who guarantees compliance with European data protection law;***
- ***Define the degree of autonomy left to the cloud service provider – acting as data processor - in the choice of methods and technical or organizational measures;***
- ***Bind the data cloud service provider – acting as a data processor - by means of a specific data processing agreement, or at least make sure that the boundaries of the data processing are clearly defined in the cloud service agreement and that the activities outsourced to the cloud service provider are adequately circumscribed;***
- ***Avoid providers who use a complex chain of sub-contractors located outside the EU.***

c. Amendments to the contract

Vendors of cloud services often include clauses in contracts whereby they retain the right to unilaterally change the cloud contract for themselves.

In legal terms, this is quite problematic and it is paramount to verify whether the contract requires the provider to give an acceptable notice for any changes to the services, or establishes the client's right to terminate the contract in face of materially detrimental changes to it.

Legal tips and recommendations:

- ***Contracts should clearly regulate which services and under what conditions, including procedural ones, can be modified in the course of the provision of services;***
- ***Changes that are materially detrimental to the level of a mission critical service or/and to the level of protection of personal data should be explicitly excluded in the contract;***
- ***Changes should not be implemented without giving notice to the client;***
- ***The written agreement of the client, or at least the client's right to be prior notified of any changes to the contract, may be foreseen therein;***
- ***The clients should verify whether the contract provides for their right to terminate it upon unwanted, unnoticed and/or detrimental amendments to the contract.***

d. Data location and transfers of data

The provision of cloud services very often entail that personal data are processed in servers, and infrastructures located outside the European Union. It is unavoidable, in this case, that personal data are transferred outside the EU. Utmost attention must be paid to the rules governing the flow of personal data from the European legal space to the outer world.

In principle Directive 95/46/EC prohibits the transfer of personal data to third countries that do not ensure an adequate level of protection for personal data.

According to Article 25 (6) «*the Commission may find (…) that a third country ensures an adequate level of protection (…), by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations (with the Commission), for the protection of the private lives and basic freedoms and rights of individuals*».[11]

As a way to derogate to the rule reported above, personal data may be transferred to countries not offering an adequate level of protection if:

- One of the conditions listed by article 26 (1) is fulfilled;[12]
- The recipients of personal data signed the standard model clauses approved by the European Commission; [13]
- The recipient organization has Binding Corporate Rules approved by the EU Data Protection Authorities in place. [14]

Transfers of data to entities established in the US are possible if the recipients are certified under the United States' "Safe Harbor" Scheme. [15]

[11] The list of Commission's decisions finding an adequate level of protection In third countries for personal data is available at the following website: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[12] «*1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:*
(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case».

[13] See Decisions 2001/497/EC and 2004/915/ EC for transfers from controllers to controllers and Decision 2010/87/EU (repealing Decision 2002/16/EC) for transfers from controllers to processors. Available at the following website: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

[14] Read here to find out more about BCRs: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

[15] Regarding the Safe Harbor, please check the official programme's website here: http://www.export.gov/safeharbor/.
However, please note 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. See the *Opinion 05/2012 on Cloud Computing, p.17, cited above.*

Legal tips and recommendations:

- ***In case the processing of personal data takes place in countries not offering adequate safeguards, both the client (controller/exporter of data) and the provider (processor/importer) must sign the model clauses adopted by the Commission with Decision 2010/87/EU;***
- ***Personal data can be freely transferred outside the EU, provided that the client verifies that one of the conditions listed above is fulfilled in the contract (i.e. article 26.1 of the Directive applies, adherence to Safe Harbor protocol etc.)***

e. Processing of personal data by sub-contractors

Providers may outsource part of the processing necessary for the functioning of the cloud to sub-contractors. These sub-contractors may receive personal data from the client of cloud services, and may be located outside the EU. They can lawfully process personal data flowing from the EU only when one of the conditions mentioned in the preceding paragraph have been met.

The chain of sub-processors may be very long and scattered, and this may result in loss of control over personal data, difficulties in the exercise of data subject's rights, and lack of accountability on the side of the data processor.

Legal tips and recommendations:

- ***In Opinion 5/2012,[16] the European DPAs recommended Processors/providers to inform the client about the sub-processing in place, detailing the type of service subcontracted, the characteristics of current or potential sub-contractors and that these entities guarantee to the provider of cloud computing services to comply with Directive 95/46/EC;***
- ***The Cloud Service Provider must ensure that its sub-contractors are contractually bound to him by the same obligations and standards he has agreed to with the controller. The model contractual clauses approved by the European Commission constitute a useful tool to this effect;***
- ***The controller should have contractual recourses against the processor in case of any breach of the contract caused by the sub-processor.***

f. Data subjects' rights (or "Intervenability")

In the framework of Directive 95/46/EC, the data subjects have the following rights:

- right of access;
- right of rectification;
- right of erasure;
- right of blocking
- right of objection [17]

When reading a cloud computing contract, the client has to check whether the provider guarantees full cooperation in ensuring an effective and easy exercise of rights on the part of the data subjects, including in cases when data is further processed by subcontractors.

[16] See the *Opinion 05/2012 on Cloud Computing, p.9, 10 and 20, cited above.*
[17] Articles 12 and 14 of Directive 95/46/EC.

Legal tips and recommendations:

- ***The contract between the client and the provider should stipulate that the cloud provider supports the client in facilitating the exercise of data subjects' rights and ensuring that the same holds true for his relation to any subcontractor.***

g. Lock-in and Interoperability

The lock-in effect may be a consequence of the cloud provider using proprietary data formats and service interfaces, which render the interoperability and portability of data from a cloud provider to another difficult if not impossible.

The lock-in effect might also hurdle the migration of services that the client developed on a platform offered by the original cloud provider (PaaS).

Legal tips and recommendations:

- ***The cloud client should check whether and how the cloud provider ensures data portability and interoperability;***
- ***Standard data formats and service interfaces facilitating interoperability must always be preferred.***

h. Service Level Agreements ("SLAs")

Service Level Agreements constitute a very important component of a cloud computing contract.

SLAs identify the services and the service level objectives that the cloud provider offers to the cloud client. The SLAs are expressed in terms of metrics on the performance of the services; the metrics are usually measured in numbers. Neither the terminology of SLAs nor the willingness to negotiate SLAs are the same between different cloud providers. This has triggered initiatives aimed at standardizing Service Level Agreements between cloud providers and clients at the European and international levels.[18]

SLAs may define the performance of the services (e.g. the availability of the service, the response time etc.), the security (e.g. service reliability, authentication and authorization, security incident reporting and management etc.), the way data are managed (data classification, data lifecycle etc.) and sometimes also relevant provisions concerning the protection of personal data.

Legal tips and recommendations:

- ***A client should attentively read and analyze the SLAs;***

[18] See, above all, the initiative undertaken by the DG CONNECT of the EU Commission that set up the Cloud Select Industry Group – Subgroup on Service Level Agreement (C-SIG-SLA) to work towards the development of standardisation guidelines for cloud computing service level agreements. The Group finalized its work in June 2014. The result thereof is available at the following address: https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines.

- *Clients should also verify whether the cloud service agreement provides for remedies to service levels breaches or if it sets out service credits for SLA breaches (such as money back rebates or monetary compensation).*

i. Termination of the contract

Termination of cloud computing contracts is a critical phase which initiates a process in which the client must be able to retrieve the data transferred to the cloud, within a specified period of time, before the provider irreversibly deletes them.

Legal tips and recommendations:

- *The steps of the termination process must be clearly identified in the cloud service agreement between the parties;*
- *A good cloud service agreement would contain provisions regulating the data retrieval time – during which the clients can retrieve a copy of their data from the cloud service - the data retention period as well as the procedures followed by the provider in order to transfer personal data back to the client or to allow the latter to migrate to another provider.*[19]

j. Privacy Level Agreements ("PLAs")

Privacy Level Agreements (PLAs) are intended to be used as an appendix to Cloud Services Agreements to describe the level of privacy protection that the cloud service provider will maintain. An exhaustive outline of PLAs has been provided by the Privacy Level Agreement Working Group established within the Cloud Security Alliance. [20]

In the PLAs the cloud service provider defines the level of privacy and protection it affords to personal data hosted in the cloud.

PLAs may tackle several issues:

- Identity of the CSP (and of Representative in the EU, as applicable), its role, and the contact information for the data protection officer and information security officer;
- Categories of personal data that the customer is prohibited from sending to or processing in the cloud;
- Ways in which the data will be processed;
- Personal data location;
- Data transfer;
- Data security measures;
- Monitoring;
- Third-party audits;
- Personal data breach notification;
- Data portability, migration, and transfer-back assistance;

[19] Also see paragraph 3.1.g. above for "Lock-In and Interoperability".
[20] See the "Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union" drafted by the Privacy Level Agreement Working Group set within the Cloud Security Alliance. The outline is available at the following website https://cloudsecurityalliance.org/research/pla/.

- Data retention, restitution, and deletion;
- Accountability;
- Cooperation;
- Law enforcement access;
- Remedies;
- Complaint and dispute resolution;
- CSP insurance policy. [21]

Legal tips and recommendations:

- ***PLAs could be used as a guide to compare the privacy policies of different cloud service providers;***
- ***PLA checklists and guidelines may be a useful tool to get acquainted with the minimum level of data protection that a cloud provider must ensure.***

4. Conclusion

Cloud computing solutions are offered in a wide variety of models, and they considerably change from one provider to another.

As already specified above, the guidelines contained herein deal with cloud computing contracts from a general perspective. From a high level they identify some of the clauses to which cloud service clients need to exercise great attention.

Solutions to the majority of issues listed in the previous pages may significantly change according to the rollout model (private, public or hybrid cloud computing) and in consideration of the deployment model (SaaS, PaaS, IaaS).

Moreover, the nature and size of both the providers and the clients has a significant influence on the way contractual clauses are drafted and viable legal solutions found.

Big clients with a considerable "countervailing buying power" are able to exert greater pressure on cloud providers. Additionally, entities such as governments, or even smaller public administrations, might have specific needs in terms of data security and business continuity because of the mission critical services they provide to the public. These are all cases that often require the provision of tailored cloud services and specific legal guidance.

Some useful legal tools are now available to the large public thanks to the effort made at the EU level under the European Commission's initiative called "*European strategy for Cloud computing – unleashing the power of cloud computing in Europe*", such as:

- **Cloud Service Level Agreement Standardisation Guidelines** - http://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines;

[21] Outline drawn from the CSA's Privacy Level Agreement Outline, cited above in footnote 20.

- **Certification in the EU Cloud Strategy** - https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy.

A further tool will be added to the "box" in 2015, when the Cloud Select Industry Group on Code of Conduct will complete its task and deliver a code of conduct for the cloud computing providers that will be submitted to the Article 29 Working Party for approval.[22]

[22] See here for more information: https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct.