Project Acronym: OPTIMIS
Project Title: Optimized Infrastructure Services
Project Number: 257115
Instrument: Integrated Project
Thematic Priority: ICT-2009.1.2 – Internet of Services, Software and Virtualisation

D7.2.1.4 Cloud Legal Guidelines Final Report

Activity 7: Business and Legal
WP 7.2: Legal Issues

<table>
<thead>
<tr>
<th>Due Date:</th>
<th>M36</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submission Date:</td>
<td>31/05/2013</td>
</tr>
<tr>
<td>Start Date of Project:</td>
<td>01/06/2010</td>
</tr>
<tr>
<td>Duration of Project:</td>
<td>36 months</td>
</tr>
<tr>
<td>Organization Responsible for the Deliverable:</td>
<td>Leibniz Universität Hannover (LUH)</td>
</tr>
<tr>
<td>Version:</td>
<td>1</td>
</tr>
<tr>
<td>Status:</td>
<td>Final</td>
</tr>
</tbody>
</table>

Author(s):
- Nikolaus Forgó (LUH)
- Iheanyi Nwankwo (LUH)
- Julia Pfeifferbrin (LUH)

Reviewer(s):
- Philip Inglesant (451 Group)
- Philip Robinson (SAP)
<table>
<thead>
<tr>
<th>Dissemination Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PU</td>
<td>Public</td>
</tr>
<tr>
<td>PP</td>
<td>Restricted to other programme participants (including the Commission)</td>
</tr>
<tr>
<td>RE</td>
<td>Restricted to a group specified by the consortium (including the Commission)</td>
</tr>
<tr>
<td>CO</td>
<td>Confidential, only for members of the consortium (including the Commission)</td>
</tr>
</tbody>
</table>
## Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments, Changes, Status</th>
<th>Authors, contributors, reviewers</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>30.3.2013</td>
<td>Initial draft</td>
<td>Nikolaus Forgó, LUH</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Iheanyi Nwankwo, LUH</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Julia Pfeiffenbring, LUH</td>
</tr>
<tr>
<td>0.2</td>
<td>12.5.2013</td>
<td>Initial draft review</td>
<td>Nikolaus Forgó, LUH</td>
</tr>
<tr>
<td>0.3</td>
<td>24.5.2013</td>
<td>Internal review</td>
<td>Philip Inglesant, 451G</td>
</tr>
<tr>
<td>0.4</td>
<td>28.5.2013</td>
<td>Internal review</td>
<td>Philip Robinson SAP</td>
</tr>
<tr>
<td>0.5</td>
<td>28.5.2013</td>
<td>Implementation of internal reviewers’ comments</td>
<td>Iheanyi Nwankwo, LUH</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Julia Pfeiffenbring, LUH</td>
</tr>
<tr>
<td>0.6</td>
<td>31.5.2013</td>
<td>Final version</td>
<td>Nikolaus Forgó, LUH</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Iheanyi Nwankwo, LUH</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Julia Pfeiffenbring, LUH</td>
</tr>
<tr>
<td>1</td>
<td>31.05.2013</td>
<td>Final overall format revision and adaptation to prepare document for submission</td>
<td>Malena Donato, ATOS</td>
</tr>
</tbody>
</table>
# Table of Contents

ABSTRACT .............................................................................................................................................. 6  
EXECUTIVE SUMMARY .......................................................................................................................... 7  
1 INTRODUCTION .................................................................................................................................... 9  
  1.1 DEFINITION, ABBREVIATIONS, ACRONYMS .............................................................................. 12  
2 CLOUD CONTRACT AND SLAS ............................................................................................................. 13  
  2.1 OVERVIEW .................................................................................................................................... 13  
  2.2 CONTRACTUAL TERMS IN CLOUD COMPUTING ........................................................................ 15  
  2.3 COMMON TERMS USED BY CSPS IN CLOUD CONTRACTS ...................................................... 18  
    2.3.1 Structure and applicable jurisdiction ....................................................................................... 19  
    2.3.2 Data subject rights .................................................................................................................. 19  
    2.3.3 Variation of terms ..................................................................................................................... 20  
    2.3.4 Data protection responsibilities ............................................................................................... 20  
    2.3.5 Localization and international transfers of data ..................................................................... 20  
    2.3.6 Use of Sub-processors .............................................................................................................. 21  
    2.3.7 Termination effects, Retention and Deletion of data ............................................................... 21  
    2.3.8 Security measures and backups .............................................................................................. 21  
    2.3.9 Liability and warranties ........................................................................................................... 22  
    2.3.10 Data breach notification .......................................................................................................... 22  
  2.4 CONCLUSION ................................................................................................................................ 22  
3 PRIVACY LEVEL AGREEMENT AND THIRD PARTY CERTIFICATION .................................................. 24  
  3.1 CONCLUDING REMARKS ................................................................................................................ 26  
    3.1.1 International Data Transfer ....................................................................................................... 27  
    3.1.2 Access by state authorities ...................................................................................................... 27  
    3.1.3 Shifting more responsibilities to the processor ........................................................................ 29  
    3.1.4 Intellectual property and the cloud .......................................................................................... 30  
    3.1.5 Cloud security standards and certification ............................................................................. 31  
    3.1.6 Green cloud .............................................................................................................................. 32  
4 FUTURE RESEARCH IN LEGAL ASPECTS OF CLOUD COMPUTING .................................................. 34  
  4.1 CONCLUSION ................................................................................................................................ 34  
ANNEX A. CLOUD LEGAL GUIDANCE FOR DATA PROTECTION COMPLIANCE ..................................... 35  
ANNEX B. LIST OF SAMPLED CLOUD PROVIDERS .............................................................................. 38  
ANNEX C. REFERENCES ............................................................................................................................ 40  
ANNEX D. LICENSE CONDITIONS ............................................................................................................ 45
Index of Figures

Figure 1. Screenshot on protection section of the programming model........................................ 11

Index of Tables

Table 1. List of Acronyms ........................................................................................................ 12
Table 2. Sampled Cloud providers........................................................................................ 38
Abstract

One of the greatest challenges facing data controllers wishing to move their data to the “cloud” is how to retain control of such data once deployed. While there is a legal requirement that data processors be contractually bound to process data according to the instructions of the data controller, the nature of cloud contracts and service level agreements make it difficult to achieve this requirement. This deliverable seeks to uncover those contractual issues that are usually of concern when outsourcing to a cloud infrastructure, and also what critical factors to consider when negotiating such a contract in order to comply with data protection requirements. Mainly focusing on those clauses that impact data protection and security, this deliverable gives insight into the risk of signing a click-wrap or standard contract drafted by the cloud service provider (CSPs) without further negotiation. In order to properly understand the issues at stake, a contract template of 15 CSPs was collected and analyzed according to the recommendations of six data protection authorities. Results obtained from this survey show that it is difficult for cloud customers to use such contracts without violating their data protection obligations, if no further amendments would be made to them. This is especially the case where all the sampled CSPs insert exemption or limitation clauses against data security breach or data loss. Our findings suggest that it will be extremely difficult to comply with regulations with such contracts, if data controllers would not negotiate some of the terms. Thus, conducting a risk impact assessment is necessary for data controllers before choosing a cloud provider. From such analysis, they will have the opportunity of uncovering high-risk areas and eliminate those CSPs that will not promote data protection compliance. Furthermore, a privacy level agreement appears to be an equally important tool at the hand of CSPs to show their level of willingness to comply with data protection principles. In addition to privacy certification, adopting a privacy level agreement will go a long way in reinforcing trust in the cloud. Therefore, it is always recommended to double-check cloud standard contracts before being bound by the terms of the contract.

Although, the OPTIMIS toolkit will be used by providers who in most cases already have their contract templates. A mechanism to include BCR and EC approved standard contractual clauses for third country data transfer has been imbedded in the toolkit programming model and SLA components. This is aimed at assisting the users of the toolkit in complying with the data protection requirements on international data transfer. Finally, as this deliverable is the last in this WP, we have annexed a concise guidance for the toolkit users and the public in general, based on our perception of the legal aspects of cloud computing.
Executive Summary

This report is the final of a four part deliverable produced in Work Package (WP) 7.2 of the OPTIMIS project. The WP focused on the legal aspects of cloud computing, and specifically considers issues of data protection, data security, intellectual property and green aspect of cloud computing. The first two reports dealt with legal requirements that will ensure compliance of the OPTIMIS toolkit with EU data protection and data security legislation, which is, ensuring that a level of data protection is maintained right from the design of the toolkit. They also presented issues relating to intellectual property and green computing. The third report centered on the technical implementation of these requirements and a license check of the toolkit components.

This final report is mainly focused on contractual and Service Level Agreement (SLA) issues in cloud services that relate to privacy. It considers how the contracts between the layers of cloud services (SaaS and Paas, Paas and Iaas) take care of data protection and data security compliance. The impact of including a privacy level agreement, as well as the use of third party privacy certification in clouds is equally looked at. The concluding part of this report however, reflects on the lessons learned on the legal aspect of cloud computing within the lifespan of the project.

Below we summarize the key points emanating from the four deliverables:

i. Moving data to the cloud does not relieve data controllers of their legal obligations, though cloud architecture and features may not allow them adequate control to fulfil these obligations.

ii. Multiple layers and actors in the cloud seem to diminish the protection of data subjects. It is not clear how the chain of contracts and SLAs used in clouds synchronize to ensure adequate protection of data subjects and to what extent data subjects can enforce their rights against these multiple actors. In a number of cases, this chain of contract is not transparent and may not be known by the cloud customer.

iii. Standard contracts as used by most CSP favour them more than the customers and from the customers' perspective, contain unfair terms in most cases.

iv. Offline and bureaucratic processes such as getting the approval from each data protection authority on each international transfer may slow down cloud activities, which intend to be automated. There is need to automate some of these compliance processes as well.!

v. Privacy by design is possible in cloud computing if it is incorporated at the design stage. This will be a good tool to enhance security and privacy such as incorporation of monitoring tools for cloud customers.

vi. The present standard contractual clauses (SCC) are not adequate in tackling all issues of international data transfers in the cloud. For instance, there is no EC approved standard contract for completing a transfer from the EU data processor to a non-EU data sub-processor. On the other hand, the new binding corporate rules (BCR) for processors will help most cloud providers who act as processors.

vii. Cloud computing can help in future energy conservation if codes of practice are adhered to. It is envisaged that there will be future legislations in this area.

---

viii. There is no standard practice at present on how to apportion intellectual property rights in the cloud. A clear definition of intellectual property rights in cloud contracts can forestall legal disputes between the cloud provider and the cloud customer. IP right clauses can be used to show what the CSP can or cannot do with information deployed or generated in the course of the service.

ix. The use of privacy level agreement and privacy certification can help cloud customers in making a good assessment of their cloud providers’ privacy protection.

x. In view of the volatile nature of cloud computing, data security requires on-going assessment. The use of encryptions, data/file segregation, data transfer restrictions, anonymization, end-to-end security of data in VM, intrusion detection, log/audit function, and backup/redundancy; are part of the mechanisms implemented in the toolkit in order to achieve a level of security.

xi. In view of the proposed Data Protection Regulation is highly recommended that a data breach notification procedure be included in the cloud contract.

Note from the authors:

We have only highlighted some of the salient legal issues in this report. For a deeper understanding of the complex legal aspects of cloud computing, we suggest reading the whole four deliverables that were complete during the project: D7.2.1.1, D7.2.1.2, D7.2.1.3 all named Cloud Legal Guidelines.
1 Introduction

In the course of this project, important documents have been published in the EU on cloud computing. The European Commission (EC), the various Data Protection Authorities (DPAs) including those of the UK, France, Italy, Germany, Ireland, etc., the Article 29 Working Party, the European Data Protection Supervisor, among others, have voiced out their opinions on the impact of cloud technology on data protection. They have also made recommendations on what data controllers should do before deploying personal data to the cloud. These opinions will definitely shape the future of cloud computing in Europe. However, what is left to be seen from these commentaries is how they will be practically implemented, especially in view of the trans-border nature of the cloud. References will be made to them in the course of this report.

That notwithstanding, a visible aspect in these publications is the recognition that the present EC standard contractual clauses are not adequate for data protection in cloud environments, indicating a need to develop new model contractual clauses for cloud transactions. The EC’s proposal in this direction is to integrate the Common European Sales Law, and other aspects of law relevant to issues of “data preservation after termination of the contract, data disclosure and integrity, data location and transfer, direct and indirect liability, ownership of the data, change of service by cloud providers and subcontracting” into such model. These issues, no doubt, are not adequately taken care of in the present EC standard contractual clauses.

One factor responsible for this shortfall is the complexity of cloud architecture and functions. Cloud services span a range of functionalities at different levels of service - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), which can be combined into one service delivery (multi-vendor integration). This integration may be complex, and although guided by Service Level Agreements (SLAs) and contracts. It is usually unclear how the layers of contract take into consideration the data subjects' interests and rights where personal data are processed. It is still unclear how to synchronize the SLAs/contracts between SaaS and PaaS, PaaS and IaaS, as well as between consumers (end users) and service providers using cloud, so as to ensure that data protection compliance, especially in the absence of a standard privacy level agreement (PLA) applicable to all the layers. Initial analysis of cloud contracts by the Cloud Legal Project indicates a lack of harmonized framework in this area. The analysis suggests that in most cases, these contracts do not meet data protection requirements. The terms and conditions offered by Cloud Service

---


5 Although cloud customers may have their own individual end users (e.g., employees or customers using the service procured) we focus only on the cloud customers' relationship with their cloud provider, not their end users.

Providers (CSPs), especially terms relating to data security and the ability to meet regulatory compliance requirements, are inadequate in most cases. These are all critical factors that should be considered by both vendors and customers alike.\(^7\)

To get an insight into the issues at stake, this report surveyed key terms taken from a range of publicly available cloud contracts (including SLAs and other Terms and Conditions from a variety of cloud service providers established both within and outside the EU market). These providers were randomly selected based on the accessibility of their contract templates and fifteen contract templates were sampled. The main focus of this survey is to see whether the publicly available contracts meet data protection requirements in view of their standard nature, and to juxtapose them with the recommendations published by DPAs. The following key provisions of cloud contracts were focused on:

(a) Data subjects as third party beneficiaries;
(b) variation of terms;
(c) data protection and international transfer of data;
(d) data security and backup;
(e) service level agreements;
(f) recovery of data arrangements;
(g) warranties and liability limitations; and
(h) (Virtualization) use of multiple parties and sub-processors in the cloud stack.

While the contracts surveyed are standard, it is important to point out that large corporate or government customers may negotiate and customize their contracts, which may not be the case for the small to medium enterprises.\(^8\) However, the Article 29 Working Party is of the view that: “The imbalance in the contractual power of a small controller with respect to large service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law.”\(^9\) Consequently, it is important that a cloud customer conducts a risk analysis before choosing a cloud service provider, especially regarding the protection of personal data and regulatory compliance.

In regard to the OPTIMIS toolkit, it is important to note here that it does not represent a stand-alone infrastructure – it has no data center of its own; rather its component will be used by infrastructure or service providers who have their standard contracts already in use. However, its design has included some restraints and easy to reach mechanisms to ensure contractual compliance for third country data transfer. A template of the EC approved model contractual clauses has been imbedded in the toolkit to facilitate the users’ compliance with EU international data transfer rules. While users of the toolkit may have their standard contracts in use, we annexed a practical guide to them when updating or negotiating their contract terms that affect data protection and security.


Figure 1. Screenshot on protection section of the programming model
### 1.1 Definition, Abbreviations, Acronyms

**Table 1. List of Acronyms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountants</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>BCR</td>
<td>Binding Corporate Rules</td>
</tr>
<tr>
<td>BDSG</td>
<td>Bundesdatenschutzgesetz (German Federal Data Protection Act)</td>
</tr>
<tr>
<td>CESL</td>
<td>Common European Sales Law</td>
</tr>
<tr>
<td>CIF</td>
<td>Cloud Industry Forum</td>
</tr>
<tr>
<td>CNIL</td>
<td>Commission nationale de l'informatique et des libertés</td>
</tr>
<tr>
<td>CSA</td>
<td>Cloud Security Alliance</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>D</td>
<td>Deliverable</td>
</tr>
<tr>
<td>DMTF</td>
<td>Distributed Management Task Force</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Network and Information Security Agency</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EUDCA</td>
<td>European Data Center Association</td>
</tr>
<tr>
<td>EuroPriSe</td>
<td>European Privacy Seal</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigations</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>Federal Risk and Authorization Management Program</td>
</tr>
<tr>
<td>FISA</td>
<td>Foreign Intelligence Surveillance Amendment Act</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>IBM</td>
<td>International Business Machines Corporation</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner’s Office (UK)</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>V&amp;V</td>
<td>Verification &amp; Validation</td>
</tr>
<tr>
<td>VC</td>
<td>Venture Capitalist</td>
</tr>
<tr>
<td>VN</td>
<td>Value Network</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>
2 Cloud contract and SLAs

2.1 Overview

In the traditional IT provisioning that occurs within an enterprise, there are usually dedicated servers and other computing resources hosted and managed within the enterprise, at least to guarantee a level of availability. This is different from the case where these servers and resources are no longer within the control of the enterprise, but managed by a contracted party. Cloud computing is an example of the latter case. As a result, this transfer of control seems necessary to guarantee a minimum quality of services from the service provider that will meet the enterprise’s requirements. This is important because the demands of the service consumers vary significantly, and it is not possible for the service provider to fulfill all consumers’ expectations. Hence, a balance needs to be struck via a committed agreement between the parties that defines the level of services offered by the provider and how they are delivered to the customer.

A Service Level Agreement (SLA) represents the parties’ consensus as to what services will be provided. Technically, it is typically expressed in a data structure that contains all the terms, guarantees and eventual penalties or rewards that the service provider and the service consumer have agreed upon. The provider of service maintains each of the SLA templates and it describes the different Quality of Service (QoS) levels and guarantees available in the service offering. A typical SLA is described using various attributes such as: availability, serviceability, performance, operations, billing, and penalties associated with violations of such attributes. The IBM review and summary of cloud SLAs for instance, states that an SLA should contain the following:

- The list of services the provider will deliver and a complete definition of each service;
- Metrics to determine whether the provider is delivering the service as promised and an auditing mechanism to monitor the service;
- Responsibilities of the provider and the consumer and remedies available to both if the terms of the SLA are not met;
- A description of how the SLA will change over time.

Legally speaking, cloud SLAs are binding contracts between a cloud service provider and a customer. Though they technically specify in measurable terms what services the cloud service provider will furnish by a set of parameters (such as the availability of the system CPU, data storage and network), violating those terms will often have some legal as well as technical

---

12 Domain agnostic templates such as the WS-Agreement and WS-Agreement Negotiation are mostly used in SLA formation, (together with a domain specific language to express QoS terms). These templates can be used in arbitrary environments, such as resource management, network management, infrastructure provisioning. There are already standardised term languages, e.g. JSDL for describing the properties of a computing job. In cloud computing, there is an activity of the Telemanagement Forum together with the Open Grid Forum, the DMTF and OASIS to define a standard for SLAs in Cloud environments. See internal communication with Wolfgang Ziegler, SLA work package team.
implications.  

SLA’s measurement of privacy level is mostly by the use of encryption, retention, deletion and isolation of data and application. There is no equivalent standardized format that holistically measures the guarantees of data protection such as regulatory compliance, return of data at the termination of services, data breach notification, access by third parties, and liability for loss of data. Currently, no “Privacy Level Agreement” (PLA) that covers data protection assurances has been adopted in the cloud environment as a clear and effective way to communicate to the cloud customer the level of data protection offered by the service provider (for evaluating whether the customer will get all the necessary guarantees to fulfill its obligations under data protection laws). PLA appears to be a prudent way of clearly defining the roles and expectations of the parties in terms of data protection compliance, where the issues are not adequately addressed in the common SLA.

Apart from the SLA, cloud customers and providers often have other contract(s)/documents such acceptable use policy, that define their legal framework. Furthermore, cloud providers may also involve multiple other processors or sub-processors, which may not be known by the customer. This is usually where transparency in cloud services is questioned because if the cloud customer is not aware of these sub-processors’ contracts, he cannot evaluate how compatible they are with his compliance obligations. As will be discussed below, some of the contractual terms used in this chain may violate data protection requirements. The French data protection authority has recognized this when it states in its recommendation that:

“[...] Cloud computing raises a number of difficulties with regard to compliance with the legislation on the protection of personal data, in particular in the case of public Cloud. These difficulties are amplified in the case of standard offers with standard contracts that customers are not able to negotiate. In general, it is found that customers suffer from a lack of transparency on the part of Cloud service providers regarding the conditions for provision of the services [...]”.

It is believed that a level of transparency can be achieved, if in addition to the common SLA, a PLA representing key privacy terms and conditions is adopted by cloud services providers as part of the contract used in all cloud transactions. The Cloud Security Alliance (CSA) has developed a PLA template based on EU data protection rules. Its adoption by CSPs will have a significant impact towards having a privacy-friendly cloud. We will further discuss PLA in chapter 5.

As will be shown below, certain provision in cloud contracts make it difficult to comply with Article 17 (3) of Directive 95/46/EC, which prescribes rules governing the contract between the data controller and the processor if those terms are not further negotiated. In most cases,

---


17 IBM, Cloud Computing Use Cases White Paper v. 4.0, op. cit., p.59.

18 In OPTIMIS for instance, data protection and privacy is also part of the SLA, e.g. by allowing the SP to require a certain level of data encryption or to restrict the provider with respect to the countries, where the data of the SP may be stored.

19 OPTIMIS for instance, embedded BCR and SCC. Documents such as cloud terms of service and acceptable use policy also form part of the cloud contract. See for example: http://www.rackspace.com/information/legal/cloud/sla (accessed 25 April 2013).

there exists exclusion or limitations of liability clauses for any security breach that goes against this provision. CNIL also finds that “in some cases of public PaaS and SaaS, customers, although responsible for the choice of their service providers cannot really give them instructions, and are not in a position to monitor the effectiveness of the security and confidentiality guarantees given by the service providers. This absence of instructions and monitoring facilities is due particularly to standard offers that cannot be modified by the customers, and to standard contracts that give them no possibility of negotiation.”

2.2 Contractual terms in cloud computing

Contractual terms used by CSPs are usually standardized for all customers, and could be gathered from different sources such as the SLA, Access Policy, Terms and Conditions of Service. Though it may be argued that standard contracts are best suited for the cloud because of the standardized nature of cloud offerings, as well as the fact that it may be difficult to change the terms for every customer without losing the most valuable advantages of the cloud, this type of contract fails to take care of individual obligations of customers from different jurisdictions. For instance, a CSP serving both US and EU customers may find it difficult developing a standard contract that takes care of the data protection requirements that differ on both sides of the Atlantic. Currently, there is confusion regarding cross-border issues of jurisdiction and applicable law, unfair contract terms, and so forth, when it is used in cloud contracts. This needs to be carefully considered to ensure consistency in cloud contracts. A possible approach to tackling the issue may be to balkanize the cloud – providing cloud services for only a particular jurisdiction or region, however such a system will invariably affect the realization of the full potential of cloud computing, and may limit the market.

Therefore, there is need for a consensus on what terms should be reflected in a cloud contract that best protect the data that are processed, no matter the location. This may indeed come from an international treaty or self-regulation as a last resort.

While there is currently no such harmonized international framework on cloud contract model, there have however been various opinions from various EU data protection authorities on what should be the essential elements of such a service contract in order to safeguard personal data. They have issued individual recommendations in this regard, and we will juxtapose these recommendations with contracts that are available in the cloud market.

Below, we give a highlight of some of the key provisions of the DPAs’ recommendations.

UK ICO

The UK Information Commissioner’s Office (ICO) issued guidance on the use of cloud computing in 2012, where it highlighted data protection issues to be addressed by data controllers wishing to use the cloud. The guidance focused on the responsibilities of data

21 Ibid, P.5.


controllers, including the requirements of a written contract. Regarding the exercise of the data subject’s rights, the ICO recommends that the cloud customer must ensure that a move to a cloud service still allows data subjects to exercise their rights. For example, that the data subjects still have a right of access to their personal data and the right to object to their personal data being processed for certain purposes.\textsuperscript{25} The guidance further states that the existences of a written contract about the service should mean that the terms of data processing operations between the parties will not be changed by the cloud provider during the lifetime of the contract without the cloud customer’s knowledge and agreement.\textsuperscript{26}

**Irish DPA**

The Irish DPA in its publication on data protection in the cloud outlines three data protection key issues - data security, data location and cloud contract - that data controllers should properly assess when moving data to the cloud.\textsuperscript{27} In order to ensure the security of the data deployed to the cloud, the data controllers is encouraged to get the following assurances from the CSP:

1. Continued access to data by the data controller (backup and disaster recovery measures);
2. Prevention of unauthorized access to data (covers both protection against external "hacking" attacks and access by the cloud provider’s personnel or by other users of the datacenter);
3. Adequate oversight including by means of contract of any sub-processors used;
4. Procedures in the event of a data breach (so that the data controller can take necessary measures);
5. Right to remove or transfer data (if the data controller wishes either to move the data back under its own direct control or move it to another cloud provider).\textsuperscript{28}

Data controllers should also ensure that appropriate measures are taken when data is located outside the European Economic Area (EEA). The written contract should be clear on the fact that the cloud provider and any sub processor used by the provider will only process data as instructed by the data controller. It should also include detailed assurance by the cloud provider on security measures, including the additional measures that need to be taken to guarantee the security of personal data that is processed outside of the (EEA).

**French CNIL**

The French CNIL has an elaborate recommendation for companies planning to use cloud computing. It includes essential elements that should appear in cloud service contract, as well as recommendation on technical and legal constraints to be considered before deploying data. The recommendation also has some models of contractual clauses on issues such as location of data, guarantee of security and confidentiality, etc.\textsuperscript{29} On using third parties such as sub-processors, the recommendation provides that the contract should include an obligation on the provider to inform and obtain the consent of the customer if third parties (sub-contractors,  

\textsuperscript{25} Ibid, p. 21.
\textsuperscript{26} Ibid, p. 12.
\textsuperscript{28} Ibid.
\textsuperscript{29} CNIL Recommendation for companies planning to use cloud computing, op. cit, pp. 2-3.
sub-providers, sub-processors) are used in the processing operation. In subsequent sub-contracts entered into by the service provider, the contractual obligations stipulated in the original service contract should be passed on to the sub-processor. There should also be provision for immediate information to the customer in case of a request from a foreign administrative or judicial authority to have access to personal data. Penalties for the violation of the SLAs should include those for the clauses on data protection (retention period, exercise of rights of data subjects, availability of processing, etc.).

**Italian DPA**

The Italian DPA advises data controllers to be conscious of the terms used in their cloud contracts, and to assess whether the terms of service are appropriate, in particular, for the obligations and liability applicable to data loss and/or unauthorized disclosure of the data kept in the cloud. There should also be a mechanism to withdraw from the service and/or shift to a different provider. Special emphasis should be put on the specifications of quality standards, and respective penalties, so that the provider is made liable for non-performance as well as for the consequences of specific events such as unauthorized access, data loss, unavailability due to malfunctioning, etc. It is also important to check whether the sub-processor is involved in delivering the services so as to put appropriate safeguards in place.

**Swedish DPA**

In one of its decisions on the use of cloud by Swedish municipalities, the Swedish DPA has stated that “unclear contracts and clauses allowing the cloud computing provider to unilaterally change the terms on which the service is provided, cause great risks since the data controller then cannot know whether it will comply with the Data Protection Act when contracting with the cloud computing provider.”

In another decision, it equally reiterates the need to name all the sub-processors in the cloud agreement. Elsewhere, it also indicated that the processor agreement must state that each sub-processor has the same obligations as the processor, issuing from the original contract with the data controller.

In the same vein, the Article 29 Working Party suggests that any such subcontract must have the consent of the data controller. Even though consent may be generally given at the beginning of the service, the CSP should have a duty to inform the client of any intended changes concerning the addition or replacement of sub-processors, and there should be at all times the possibility for the client to object to such changes or to terminate the contract. This is also in line with the UK ICO’s recommendation that in the case of layered services, the cloud provider must keep the cloud customer informed of changes in the chain of sub-processors that are used in the course of providing the cloud service.

---

33 Ibid.
36 ICO, Guidance on the use of cloud computing, op. cit., p.12.
German DPAs

Like the French CNIL, the German DPAs also have a detailed guide on the necessary content of a cloud contract. The guide considers the cloud customer as a data controller, and the cloud provider as a data processor, so that the contract must comply with the special requirements for data processing as required by Article 17 of the Data Protection Directive and § 11 of the Federal Data Protection Act (BDSG). The contract among other things must ensure that the provider is obligated to support the cloud user with the enforcement of data subject rights (right to information, correction, blocking and erasure). All locations used for data processing as well as all sub-processors should be named in the contract. Penalties against the provider or sub-processors could also be stated in the contract as a mechanism to enforce their obligations.

Standard contractual clauses and binding corporate rules can be used to legalize international data transfer. There is also guidance on security risks of using a cloud service and the technical and organizational measures to be put in place, especially when using a shared infrastructure. The contract must contain appropriate control and auditing functions to enable the cloud customer to monitor the provider’s compliance with the contracts, as well as include a data breach notification clause.

2.3 Common Terms used by CSPs in cloud contracts

As earlier indicated, there is no global standard contractual model for effecting cloud services between cloud customers and their CSP. A study by the Cloud Legal Project found that about a half of sampled cloud customers could not negotiate their terms and conditions with their cloud provider and ended up accepting the standard contract. This study concludes that these contractual terms favor the cloud providers to a great extent, and a similar conclusion was also reached in a 2011 survey by the Cloud Industry Forum.

Below, we will examine these standard terms and conditions to evaluate whether they meet data protection requirements, especially, in view of the various DPA recommendations above. The terms analyzed here are those published on the website of the CSPs we investigated, though we recognize the fact that some parties may modify their contracts if negotiated or can be amended through customer’s orders. However, we have focused on the publicly available templates, assuming that they would be used in a real contract without modification.

40 http://www.cloudlegal.ccls.qmul.ac.uk/
42 Ibid, p. 83.
44 A table containing the examined CSPs can be found in Annex A to this report.
45 One of the limitations we encountered in the course of the survey was to find all relevant documents relating to the contract between a user and a provider on the Internet. Some providers do not even publish any terms of service on their website or they are so well hidden that it is almost impossible to find. Others include extra documents such as special terms of use for different services, additional privacy or trademark policies, acceptable use policy or general terms of service, which can replace or change some clauses in the “original” contract.
Another assumption we make in this survey is that we regard the cloud providers as data processors (that is, not as "data controllers"), which is relevant to the issue of compliance with Article 17 of the Data Protection Directive, especially the control possibilities of the data controller over the data processor.\footnote{However we recognise the fact that there may be cases where the CSP may be a data controller, see Article 29 Working Party, op. cit} This means that the customer, as data controller, is responsible for data protection, and that the cloud computing contracts ought to contain a clearly identifiable component that constitutes a processor agreement. We seek to determine whether the contract templates resemble these control possibilities for the customer, and in doing so, the following terms were considered:

### 2.3.1 Structure and applicable jurisdiction

The reviewed cloud service providers do not offer a single contractual document about their cloud services, but use several documents such as General Terms and Conditions, Service Descriptions, Special Terms for Services, SLAs, additional Privacy or Trademark policies or additional Security Descriptions, which could modify or amend the general contractual document. Some CSPs have these documents cross-linked in the general contract template, which makes them relatively easy to find. Some others do not have these links, or do not even make easy references to them. An example is Microsoft’s Azure, where the use of EU Model Contract clauses is only mentioned in their Trust Center Privacy page\footnote{http://www.windowsazure.com/en-us/support/trust-center/privacy/ (accessed 27.05.2013).} without a direct link to this information in the Agreement.

Differences also exist in the structure and length of contract templates between different providers. Amazon’s terms of service (“AWS Customer Agreement”) for example, is quite short and does not differentiate between the different countries and jurisdictions.\footnote{AWS Customer Agreement, Section 13.11 (http://aws.amazon.com/de/agreement/) (accessed 23 April 2013).} IBM on the other hand provides, in Part 2 of its agreement for the Enterprise Smart Cloud, different country-specific clauses that take into account specific national jurisdictions and legal requirements for contractual obligations.\footnote{http://www-935.ibm.com/services/us/en/cloud-enterprise/contracts/sc_agreement_sign.html (accessed 23 April 2013).} For instance, it uses a special liability clause for German contracts since it is not allowed in Germany to exclude all liabilities in a contract. IBM’s agreement also goes further to state the applicable law (country-specific) for the contract.

### 2.3.2 Data subject rights

Data subjects’ rights - information about processing, erasure, and so forth, - are core data protection requirements in any personal data processing. As stated by the UK ICO, the obligation is on the cloud customer to ensure that a move to a cloud service still allows data subjects to exercise their rights, and this should of course be reflected in their cloud contracts. Of all the contracts surveyed, four providers declared their obligations to support the customer with his duties. For example Microsoft uses an additional “Data Processing Agreement” as part of its contract framework, where it promises to support the user, if he has to enforce his rights:

For the duration of Microsoft’s provision of the Services to Customer, Microsoft will, at its election and as necessary under applicable law implementing Article 12(b) of the Data Protection Directive, either: (1) provide Customer with the ability to correct, delete, or block
Customer Data it provides to Microsoft through the use of the Services, or (2) make such corrections, deletions, or blockages on Customer’s behalf.50

While the EC standard contractual clauses have third party beneficiary rights for the data subject, none of the contracts surveyed granted it.

2.3.3 Variation of terms

The cloud provider’s right to change the terms of service unilaterally was found in all the terms of service surveyed. However, in most cases the customer can terminate the contract if he does not accept the changes. Nevertheless, differences exist as to whether and how the customer would be informed about the changes (only on website or through email) and how much time is granted before the changes would apply. It should be noted that without efficient notification of such changes to the customers, it would be difficult for them to recognize any changes that could affect their data protection obligations. This term diminishes the required control over the cloud provider contrary to Article 17 of the Directive51.

2.3.4 Data protection responsibilities

All but one of the sampled CSPs state that they are only data processors and that the customer is responsible for complying with the relevant data protection regulations. Only Rackspace implies in its template that it in some circumstances it would be a data controller as well as, or instead of, being a processor, but without any clarification as to when this can happen.52 While most of the cloud providers may be processing data on behalf of the data controllers, it is not clear how instructions are passed to them as processors and much control the data controllers have over them as required by the Directive.53

2.3.5 Localization and international transfers of data

Differences also exist about information on the localization of the data centers. Some CSPs provide the so-called regions, which can be chosen by the customer, so that data transfers will be carried out only within the selected regions.54 But the concrete location of each data center is not described in the contract. It is also not indicated in the contracts under which basis a data transfer to third countries would happen. Some providers simply offer to transfer data only to those sub-processors who have an adequate data protection level, but without explaining how they arrive at the adequacy protection levels. Not all of the reviewed templates did indicate directly in the contract if they use the standard contractual terms or Binding Corporate Rules to achieve an adequate level of data protection for international transfers. Google Apps55, Microsoft Office 365 solution, and Microsoft Azure use European Model Contractual Clauses56 as shown on their websites.

53 See for example Article 17 of the Data Protection Directive.
54 For Example Microsoft Azure, Amazons AWS and Google provide such European regions.
2.3.6 Use of Sub-processors

All providers have reserved the right to use sub-processors to offer parts of the service, including the right to transfer data to them, even when they may be located outside the EEA. Most of the cloud providers declare themselves to be responsible for their sub-processors and to bind them in a contract equal to the one between the provider and the customer. However, of all the surveyed providers, only one provider (SAP) offered directly in the contract to reveal names, addresses and role of all sub-processors to the customer in its Terms and Conditions. In general, it appears that a customer would know that using a sub-processor is possible, but might not know who the sub-processor is, and whether such a sub-processor is qualified to do the processing. European DPAs require that the name and data center locations where all sub processing are carried out be revealed to the cloud customer. However, this seems not to be the case presently.

2.3.7 Termination effects, Retention and Deletion of data

Another important clause in cloud contracts is the retention or deletion of content data when the contract is suspended or terminated. Most providers did not specify in clear terms their rights and obligations regarding the deletion or retention of data when the contract ends. Usually the contracts simply state that data could be deleted after a specific duration, but not that the CSPs have an obligation to delete them. In most cases, customers can only get back their data after a termination if they have paid for the service and do not have any open bills with the provider or both. Requiring payment before data is given back can lead to a loss of personal data if the cloud user is in financial difficulties.\(^\text{57}\) It is also important to look at the reasons to terminate or suspend a customer’s account by the cloud providers. Some providers reserve the right to suspend or terminate the account if they believe the customer has violated the Acceptable Use Policies or the contract.\(^\text{58}\) Without any obligation to notify the customer prior to such suspension, this could result to inability of data subjects to access their personal data. Only one provider stated clearly the format it would return data and only four contain a clear obligation to return stored data to the customer.

2.3.8 Security measures and backups

The description of security and organizational measures to protect stored data is also differently stated among the reviewed CSPs. A reason therefore could be not to reveal too much security information about the data centers and software to an unknown public. While nine providers gave scanty information about their security measures in the contract template, six other providers included detailed descriptions of their security mechanism in the general contract, or make a reference to their security website where these are described as well as the certificates they obtained. But it has to be noted that security requirements depend also on the services in focus. For example, an IaaS-provider only offers the hardware infrastructure, and has no influence on the used software. In this case it seems appropriate that the customer is responsible for the security measures within his own space. On the other hand, in a SaaS-cloud, the customer has no control or influence on the security measures over the used hardware and software. Similarly, it is also not in every case that the provider agrees to keep backups for the customer. Customers are sometime left to take care of backup. Nevertheless, some providers offer it as an extra service with charge, while some others occasionally offer it


without any binding obligation - five of our reviewed contracts contain such a possible service but without any obligation on the provider.

2.3.9 Liability and warranties

Cloud providers exclude or limit the liability to a specific amount for the loss of data or content from their contract, and this could become critical for the customers because the main purpose of using cloud solution is the processing or storing of customer’s data. A similar picture exists with warranties. Most Providers do not give any warranties except those in the SLA about availability of the service. Exclusion of liability in these cases means that the data controllers will remain liable for the errors or negligence of the CSP, even when they do not have control over the CSP’s activities.

2.3.10 Data breach notification

The DPAs and the Article 29 Working Party have recommended that providers notify their customer about data protection violations (“data breach notifications”). But most of the reviewed contracts do not have strict obligation for this. One provider however, declared that it would notify the customer immediately about suspected data protection violations. Some other providers would grant such notification obligation only when required by law.

On the other hand, all providers demand from their customers to notify the cloud provider as soon as possible if an unauthorized person gets access to the cloud service, which means that the customer has the strict duty to notify the CSP about misuse or unauthorized access to data. It is crucial for a clear duty of notification to be included in the contract, because data breach notification is important for the customer, as the data controller who is has obligations under certain national laws, and the proposed data protection Regulation, to report such violation of data protection to the supervisory authority and the concerned data subjects.

2.4 Conclusion

From the analysis above, it could be deduced that certain contractual clauses and standard terms of service used by most cloud providers do not comply, in most cases, with the requirements of the Data Protection Directive and national data protection laws. It was found that these standard contracts do not reflect a huge power imbalance between the customer and the CSP. There is a large gap between the existing contracts and the DPAs’ positions outlined above. Standard terms excluding liability and warranties, for example, are frequently inserted into the contract, which is to the disadvantage of the cloud customer. The possibility for the data controller to control the processing is made more difficult where the CSP uses multiple sub-processors to offer the services, who often are located in multiple jurisdictions. Similarly, the ability of the CSP to unilaterally modify the contract means a further loss of control on the part of the customer, if this is not properly brought to his notice so as to take a proper action. In most cases, no clear obligation exists to return and delete data when the service is terminated or suspended. This could become critical for the customer if the provider terminates access to the service.


60 For example see § 42a German Federal Data protection Act.

61 Art. 31 (1) of the proposed General Data Protection Regulation, COM(2012) 11 final.
The presumption that data controllers have power to instruct the data processors may be incorrect in cloud services as reflected in the power imbalance in favor of the CSP. While cloud customers are responsible as data controllers, they do not have the bargaining power to detect how the processing is done in most cases. This then raises the questions whether it is possible to use cloud computing and still comply with data protection obligations, if customers are not able to negotiate terms with providers. In our view, without further negotiations on these terms, it will be difficult for data controllers to meet their compliance obligations.\textsuperscript{62}

3 Privacy Level Agreement and Third Party Certification

The preceding chapter shows the impact of lack of harmonization in cloud contracts on privacy and data protection. While certain efforts have been made at getting a global standard in this regard, success has been limited due to a number of issues such as jurisdiction.\(^{63}\) That notwithstanding, there have been industrial initiatives aimed at defining privacy level for CSPs.\(^{64}\) The Cloud Security Alliance (CSA) for example, has been working on defining baselines for compliance with data protection legislations and best practices in a standard PLA, through which a cloud service provider could declare the level of privacy (personal data protection and security) that it sustains for the data processing.\(^{65}\) Its PLA Working Group recently published a PLA outline for the sale of cloud service in the EU that is based on the EU and the OECD privacy principles. This initiative has the following objectives:

A) To provide cloud customers with a tool to assess a CSP’s commitment to address personal data protection.

B) To offer contractual protection against possible economic damages due to lack of compliance or commitment of the CSP with privacy and data protection regulations.

C) To provide the CSP with a tool for structured disclosure of its privacy and data protection practices.

It has developed 16 core fields that a CSP should reflect in its privacy agreement with the customer,\(^{66}\) and the Working Group hopes that the adoption of a common structure for PLA worldwide could be a powerful industry standard and a self-regulation tool that may enhance adherence to, and compliance with applicable data protection, transparency and accountability obligations as required by EU law. We assess this as a good development in achieving a level of privacy and transparency in cloud services. Hopefully, this will form a good basis for reforming the standard contracts as currently used in the cloud market, as well as being a step towards creating publicly available cloud offerings that meet European standards.

Apart from the PLA developed by the CSA, there have also been suggestions that independent third party certification of CSP privacy level should be used as an objective tool for evaluating cloud provider’s privacy compliance. Independent certification by a reputable third party could be a credible means for cloud providers to demonstrate their compliance with data protection principles. This could also be an avenue for customers planning to use cloud services to check whether their intending cloud provider(s) can provide a level of privacy compliance. The EC seeks to utilize this medium as one of its key action plans for unleashing the potential of cloud. In this respect, certification of cloud services will indicate that they meet certain standards, and the endorsement of such certificates by regulatory authorities will further indicate compliance with regulatory requirements.\(^{67}\) The EC plans to work with the support of ENISA and other relevant bodies in developing an EU-wide voluntary certification schemes in the area of cloud computing (including data protection) and establish a list of such schemes by 2014.\(^{68}\)

Although there have been a number of certifications of security compliance for cloud providers such as the Payment Card Industry Data Security Standards (PCI-DSS), ISO 27000 series, the

\(^{63}\) See for example: Cloud Standards Customer Council.

\(^{64}\) See the activities of the Cloud Security Alliance (CSA), https://cloudsecurityalliance.org/ (accessed 12 April 2013).


\(^{66}\) See the Privacy Level Agreement (PLA) Outline Annex.

\(^{67}\) European Commission, Unleashing the potential of cloud, op.cit, p.10.

\(^{68}\) Ibid, p.11.
Unified Certification Standard, CIF, and so forth, only a few of these schemes have centered on the privacy level. Currently, privacy certification initiatives for cloud providers include the European Privacy Seal (EuroPriSe), TRUSTed Cloud Data Privacy Certification from TRUSTe data privacy management solutions provider, and the US-EU Safe Harbor Certification. The EuroPriSe is an initiative that offers certification to manufacturers and vendors of IT products and IT-based services that meet EU privacy standards. Cloud service providers can be EuroPriSe certified, where the contractual safeguards of the client-provider relationship deals with the following issues to ensure legal certainty, and in compliance with Article 17(3):

1. Details on the cloud client’s instructions to be issued to the cloud provider, with particular regard to the applicable SLAs and the relevant penalties
2. Specification of security measures that the cloud provider must comply with - it is of great importance that concrete technical and organizational measures are specified
3. Subject and time frame of the cloud service as well as extent, manner and purpose of the processing of personal data and the types of personal data processed
4. Specification of the conditions for returning personal data or destroying the data once the service is concluded
5. Inclusion of a confidentiality clause, binding both upon the cloud provider and any of its employees who may be able to access the data
6. Obligation on the cloud provider’s part to support the client in facilitating exercise of data subject’s rights to access, correct or delete their data
7. The cloud provider may not communicate the data to third parties, unless it is provided for in the contract that there will be subcontractors (NB: The contract should also stipulate the legal safeguards that are mentioned below under “Subcontractors”)
8. Clarification of the responsibilities of the cloud provider to notify the client in the event of a data breach which affects the client’s data
9. Obligation of the cloud provider to provide a list of locations in which the data may be processed
10. The cloud client’s rights to monitor and the provider’s corresponding obligations to cooperate
11. The cloud provider must inform the client about relevant changes concerning the respective cloud service such as the implementation of additional functionalities
12. Logging and auditing of relevant processing operations on personal data that are performed by the cloud provider or the subcontractors
13. Duty of the cloud provider to notify the client about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation and the duty to reject any non-legally binding requests for disclosure

---

14. A general obligation on the cloud provider’s part to give assurance that its internal organisation and data processing arrangement are compliant with the applicable legal requirements and standards.

TRUSTed Cloud Data Privacy Certification is also equipped to certify the privacy practices of cloud companies and can help them reassure clients and customers of the strength of their data management practices. TRUSTe privacy certification programs are comprised of program requirements that define a compliance standard for business practices involving the collection and use of data. To obtain TRUSTe certification, a company must provide proof of its privacy and data governance practices for data collected on behalf of users, customers, and partners - particularly as these practices relate to notice, choice, and accountability.

The Safe Harbor certification, as created under the EU-US Safe Harbor Programme, is another important privacy enhancing scheme. Companies in the US that wish to process personal data from the EU are expected to obtain such a certification annually as evidence of their compliance with the Data Protection Directive. Any company that fails to renew its certificate automatically loses the Safe Harbor benefits.

3.1 Concluding remarks

With the potential of cloud still under discovery, governments and businesses are shifting their policy from dwelling on the risks of using the cloud to adopting a cloud strategy. The UK government, for example, has shown remarkable commitment to adopting greater use of cloud services in its G-Cloud programme, which has put together a catalogue of cloud information and communications services available to the UK public sector. France, Germany and many other EU Member States have also adopted different strategies for promoting the cloud computing within their jurisdiction. Similarly, a good number of regulatory authorities are finding ways to accommodate the use of cloud. The Norwegian DPA recently shifted grounds by giving a qualified approval to all local municipalities to use Google Apps and Microsoft's Office 365. The Dutch Central Bank has also concluded an agreement with Microsoft over auditing rights in its Office 365 cloud service contracts, which was difficult to negotiate by the individual financial institutions. This positive participation of governmental authorities in the cloud ecosystem will definitely change the attitude of users outside government towards its adoption.

In the course this project, many lessons have been learnt about the legal aspects of cloud computing: even though some may downplay the significance of the emergence of cloud, others believe it is yet another area of the application of ICT that has major repercussions on legal regimes. This debate will continue, but one thing that is noticeable is that certain legal principles (including data protection rules) may be difficult to apply in a cloud environment without some modifications. A typical example will be the controller-processor dichotomy as used in the current Data Protection Directive and the assumption that the data controller has a

---


reasonable control over his appointed data processor. These established principles may not fit in well with the multiple actors seen in the cloud ecosystem such as cloud brokers, cloud integrators, etc. The Queen Mary University Cloud Legal Project has been current on these issues.\textsuperscript{77} We give below a summary of the core issues in legal discussion of cloud computing as uncovered in our research in the project:

3.1.1 International Data Transfer

One of the issues that will continue to be in focus in cloud discussions is how to regulate international data transfers. One EU press release notes in this direction that: “There are no borders online and cloud computing means data may be sent from Berlin to be processed in Boston and stored in Bangalore.”\textsuperscript{78} This will have an impact on data protection, especially on the need to protect personal data, so that such data benefits from the same level of protection accorded to them from their country of origin. The EU for instance has a very strong data protection law, which forbids the transfer of data to third countries that do not offer adequate level of data protection. While some have suggested that the best way to tackle this problem is by building a European cloud, so that data that originate from Europe will stay within its cloud, this may mean a balkanization of the cloud ecosystem, without reaping its full benefits.

Tackling this problem will require an international approach, for instance, a treaty that will set a common standard applicable to any state where cloud data moves. This may be difficult to achieve in a short term, but will definitely bring a level of legal certainty in this area. Though common approaches such as the EU framework of using Standard Contractual Clauses (SCC) and the Safe Harbor have been adopted for cloud transactions, it is not clear how the long arm of these arrangements will be enforced against numerous sub-processors who are involved in cloud services, and who in most cases are outside the applicable jurisdiction.

Secondly, the problem of balancing bureaucratic processes when getting approval for BCR or for data export under the current data protection laws needs to be addressed. Automated processes as envisaged in cloud computing may be delayed when complying with these processes; to provide adequate response times, such systems also need to be automated in future. In OPTIMIS, an automated platform has been created where the SCC and Binding Corporate Rules (BCR) could be effected electronically, nonetheless the offline processes, such as initial approval of the BCR, would still need to be handled manually. While the proposed data protection regulation will harmonize issues of multiple approval processes (creating a one-stop-shop), there is also the need for automated processes such as verification of the Safe Harbor certification status of a US company. This will ensure that companies listed in the Federal Trade Commission (FTC) website claiming to be certified are genuinely certified, and will create a level of certainty as well as hasten the process of such verification.

3.1.2 Access by state authorities

One important other consideration relating international transfers of personal data is to what extent the state authorities such as law enforcement agencies could get access to data stored or processed in the cloud within their jurisdiction. A recent study on behalf of the European Parliament finds that the risks and dangers of cybercrime are not the most pressing in the cloud, but those of loss of privacy, especially disclosure of data to foreign governmental

\textsuperscript{77} http://www.cloudlegal.ccls.qmul.ac.uk/ (accessed 22.03.2013).

authorities on the basis of legislative instruments, such as the US Patriot Act and Foreign Intelligence Surveillance Amendment Act (FISA). Such instruments include obligations on cloud providers to grant access to any data stored in their cloud to governmental authorities for criminal investigations. Microsoft’s admission of its obligation to disclose data in its cloud under the US Patriot Act has often been cited to buttress this issue. The FBI for instance can pass access orders directly in some cases, without a court review (National security letters). The implication of the above may be that when using a US-based cloud provider, a disclosure to US authorities maybe possible and lawful under US law, even if the provider stores data in data center in the EU. This risk also exists even when the EU-based cloud provider has offices or a systematic business relationship in the US.

However, it has to be stressed that apart from what has been pointed out above, a disclosure of European cloud data could also take place on the basis of Mutual Legal Assistance Treaties (MLAT), which are signed between other countries and EU Member States. For example, the German government reported that it has transferred and requested data to and from the US authorities on basis of MLATs. Similarly, a white paper from Hogan Lovells (2012) has also pointed out that many other jurisdictions apart from the US government equally have such access rights legislations. Microsoft and Google published their Legal Enforcement reports for 2012, which show that other governments request customer traffic and, sometimes, content data. Germany has been shown to request data from Microsoft in 8,419 cases. A possible conclusion to reach from the above is that foreign governmental authorities can get access to cloud data on multiple different legal grounds. This could place some cloud providers in a difficult position of violating data protection laws, and there is need for an international harmonisation of laws on granting state authorities access to data originating from other jurisdictions that are stored or processed in the cloud.

3.1.3 Shifting more responsibilities to the processor

Under the current Data Protection Directive, data controllers have significant duties and obligations, and are liable for any act or omission with respect to personal data in their custody. They must comply with rules on how to collect or use personal data, and are responsible for any use of these personal data by their processors. On the other hand, data processors are not primarily liable for failure to comply with the Data Protection Directive. They are assigned with only a small amount of responsibilities, and/or contractual obligations that pertain to keeping personal data secure from unauthorized access, disclosure, destruction, or accidental loss. Thus, the status of an entity processing personal data has significant consequences. CSPs regard themselves as data processors and this has major implications in terms of obligations and responsibilities under the EU data protection regime. As evidenced in the cloud contracts reviewed above, this places on the customer the entire burden of compliance with the applicable data protection requirement.\(^{87}\)

One of the risks associated with relinquishing control to data processors in cloud computing is that there is no corresponding shift in legal responsibility when CSPs are merely regarded as data processors. This means that in most cases, the data controllers will be held fully liable for the acts or omissions of their CSPs,\(^{88}\) and there is ample evidence that data breaches or losses of personal data have been caused by the actions of data processors. This imbalance has led to suggestions that in some cases, CSPs should be regarded as a data controllers or joint controllers despite the wording of their contract with their customers;\(^{89}\) it is however not certain how this will be resolved in practical terms when disputes arise.

In the same vein, it has equally been suggested that greater compliance responsibility be imposed upon cloud data processors, so as to reflect their level of control. This would mean that some of the exclusion clauses as used in cloud contracts would not have any legal effect, as they would then be contrary to the processors’ legal obligations. The proposed General Data Protection Regulation, when it becomes enforceable, however, will increase data processors’ obligations, as reflected in the following provisions:\(^{90}\)

a) Article 26 which provides that if a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllership, which have some onerous provisions relating to data subject access.

b) Article 28 obligates a processor to maintain documentation of all processing operations under its responsibility.

c) Article 30 requires data processors themselves to implement and maintain technical and organizational measures to keep the data they hold secure, and to prevent unlawful destruction or accidental loss as well as unlawful forms of processing such as unauthorized dissemination and access. This obligation is subject to the nature of the data held, and is to be proportionate to the cost of such measures. Nevertheless, the requirement is directly enforceable against data processors.

---


\(^{88}\) Ibid

\(^{89}\) For a full discussion on this, see D7.2.1.

\(^{90}\) These provisions are based on the draft of the Regulation released by the European Commission in January 2012.
d) Article 31 indicates that the processor shall alert and inform the controller immediately after the establishment of a personal data breach.

e) Under Article 35, all organizations with 250 employees or more, or whose core activities consist of processing operations which require regular and systematic monitoring, and all public authorities, that control or process data must designate a Data Protection Officer (DPO) who shall be responsible for compliance. The data processor and data controller may however, appoint a joint DPO.

f) Most significantly, data processors may now also be directly liable for any sanctions that are imposed by the competent regulating authority for intentional or negligent failure to comply with the regulation, such as monetary fines, imposition of a ban on processing, or order to destroy data.

This is a welcome development, as it will place greater responsibility for data protection onto data processors. Individuals will also have the right to sue a data processor for compensation in view of any damage suffered as a result of unlawful processing of data by the processor; it is hoped that this will significantly improve the negotiating powers of data controllers in cloud service provisioning, and will mean that some of the exclusion of liability clauses will not be effective in the future.

3.1.4 Intellectual property and the cloud

Intellectual property (IP) issues (copyright, patent, trade secret, etc.) have also been considered in a number of discussions about cloud. Two distinct areas are of concern here: issues relating to ownership and use of IP created before moving to the cloud; and metadata associated with the use of the cloud, that is, information generated with the cloud infrastructure while the services are running, such as logging information, billing data, information generated through mining, etc. While it is generally agreed that deploying IP-related information to the cloud does not, and should not, deprive the rights holder of their IP entitlement, it is not clear how information generated while the service is running should be allocated property rights in a number of instances. Clearly, if the CSP has generated the data for its internal purposes such as billing, the IP rights no doubt belong to the CSP. However, how to allocate certain data, such as traffic data or data generated through mining that are relevant to the cloud customer’s activities, is still unsettled. Can the CSP distribute (voluntarily or otherwise) such metadata, which may affect the customer and their end users? A similar issue is how confidential data such as trade secrets are protected in the cloud. Does the duty of confidentiality extend to sub-processors who are engaged by the service provider? And what happens if the cloud services are terminated?

While the resolution of the above issues may be complex, one possible way of addressing them appears to be through a good contract that clarifies and makes explicit the limitations of data usage and ownership rights. Such a contract should for example, limit what the CSP could do with the data generated through its infrastructure such as mining or any other exploitation. Gartner’s Global IT Council for Cloud Services concludes that the service consumer has the

---


right to retain ownership, use and control his or her own data, and that this will help establish and maintain successful business relationships with the cloud provider. But experience has shown that the standard contracts do not take care of these issues. Therefore, due diligence is required when choosing a cloud provider. It is also important that both parties obtain requisite licenses that will allow the smooth performance of the cloud services to avoid infringement of third party rights.

### 3.1.5 Cloud security standards and certification

Although some analysts argue that CSPs could provide more security for data within their clouds and are in a stronger position to do so owing to their much larger resources and expertise compared with SMEs, it is not entirely clear how this translates into the implementation of Article 17(2) of the Data Protection Directive 95/46/EC. The Directive puts full responsibility on the data controller to choose a processor to implement adequate technical and organizational security measures to protect personal data and also to be able to demonstrate accountability. Factors to be considered in making this choice are not expressly provided in the Directive, which raises the question whether information security standards such as the ISO /IEC 27001: 2005 could be seen as state of the art in ICT, and what would be a common security standard for cloud computing. Can we really be sufficiently certain about the risks involved in a cloud service as to be able to specify what technical and organizational measures must be put in place? Security breaches witnessed frequently in the cloud suggest that this is unrealistic.

On the one hand, cloud providers may not easily provide each customer with an avenue for deep inspection of their security mechanisms, as this could also increase their security risk. Certification of cloud services, on the other hand, for verification of the security level of a provider, could be a tool to enhance acceptance and transparency in this domain. Such schemes could also help providers to clarify what adequate technical and organizational measures to be implemented, as the current Directive 95/46/EC does not provide any specifications on this area. A large number of certifications and standards exist today in the cloud domain such as the ISO 27001 series, Service Organization Control (SOC) 2, the SSAE 16 standard (former known as SAS 70), PCI-DSS, etc. The PCI-DSS for example, is a standard for services which are using a credit card management system. Apart from self-certification, some sector-specific regulations are evolving, such as the US Health Insurance Portability and Accountability Act (HIPAA) (for services which are dealing with electronic health information) and the FedRamp Program (for cloud solutions used by US-governmental authorities) which seek to impose certain standards for cloud providers.

However, it has to be stressed that although certificates can help cloud customers to assess a cloud provider, no one certificate may cover all areas, which are relevant to the customer. Providers do not need to certify their whole service offering, so just a part of an offered solution can be certified. Furthermore, despite the fact that certifications are increasingly used

---

97 Ibid.
in the area of privacy such as the Trusted Cloud seal by TRUSTe,100 EurpriSe seal101 and the EuroCloud Star Audit,102 it has to be noted that these certificates are not backed by any specific legislation, which may have the implication that such independent third party certificates may not be seen as adequate to show compliance with the Data Protection Directive 95/46/EC.

Besides the security standards mentioned above, hardware or software standards in cloud solutions are still evolving, which means that cloud data or applications from one cloud provider may not work properly in another cloud solution. Several initiatives and projects are working on developing common standards or frameworks for cloud solutions to increase the interoperability between different cloud providers, such as the National Institute of Standards and Technology (NIST).103 The absence of such interoperable standards could lead to vendor lock-in or at least requiring a significant effort for the customer to retrieve their data in a usable format.104 The EC has observed this, and proposes to develop necessary standards in this respect.105 Interoperability will be a topical issue in the near future in view of the proposal in the new Data Protection Regulation that grants data subjects the right of data portability. This means that data subjects will have a right to retrieve their stored data from the data controller in an electronic and structured format which is commonly used and allows for further use by the data subject.”106 This will play a relevant role in cloud adoption in the future.

3.1.6 Green cloud

A number of research findings suggest that cloud offers the potential of reducing energy consumption and carbon emissions. A white paper from Google indicates that a typical company or organization that migrates to the cloud could save an estimated 68–87% in energy for its office computing and could also reduce similar amounts of carbon emissions.107 A similar result was obtained in a study of Microsoft cloud solutions.108 These indicate that through the use of large shared servers and storage units, cloud computing can offer significant energy savings in the provision of compute and storage services. Moreover, companies migrating to cloud services will in turn run fewer servers on-premise, potentially leading to a further reduction in pollution.109

However, it has to be pointed out that cloud computing also leads to increases in network traffic and the associated network energy consumption as a result of the increase in size and capacity of data centers and of networks; overall energy savings can only be achieved if this is properly managed.110 Due to the large number of equipment, data-centers can consume

---

104 European Commission, Unleashing the potential of cloud , op. cit, p.10; Art.29 Working Party, WP 196 op. cit, pp. 5 - 7.
105 European Commission, Unleashing the potential of cloud, op. cit, pp.10, 11.
106 Article 18 (1) of the draft Data Protection Regulation.
110 Ibid.
massive amounts of energy and emit a large amount of carbon.\textsuperscript{111} There is, however, the prospect that utilizing advanced data center infrastructure designs that reduce power loss through improved cooling, power conditioning, and so forth, can reduce their carbon emission.

In D7.2.1 we enumerated the initiatives on green cloud, and at the European level, a code of conduct for data centers was released by the EC in 2008.\textsuperscript{112} The European Data Center Association (EUDCA)\textsuperscript{113} has also set up four working groups to address specific issues relating to the data center industry at a European level. The Energy Working Group is looking at the energy policy of the European data center industry in a bid to reducing energy consumption. While these efforts are commendable, it is important that the cloud industry emulate the OPTIMIS initiative, which includes eco-efficiency as one of its TREC factors. Where this approach is sustained, using the cloud will significantly make the environment better by reducing carbon emission.


\textsuperscript{113} European Data Center Association, http://www.eudca.org/home.
4 Future research in legal aspects of cloud computing

Our inquiries suggest that there is still need for a continuous legal research on the impact of cloud computing to data protection and data security. The Cloud Legal Project\(^{114}\) being undertaken by the Queen Mary University in UK is a good step towards understanding the architecture and impact of cloud from a legal perspective. This will no doubt assist policy makers in developing the right regulations for the cloud. However, there are still problems in applying certain data protection principles in the cloud. This requires further research. The cross-border nature of the system requires an international approach in a number of cases. Legal research need to be done to determine whether and how cloud computing risks could be reduced through an international treaty.

Another area for future research will be to determine whether regulation for data protection in the cloud should be more sectors specific. In the United States for example, such sector specific regulations exist such as the HIPAA framework the health sector, or the FedRamp program for federal institution or the PCI for the financial sector. While it may be debated if such specific sector regulations for all areas of possible cloud solution is feasible, such an approach could create better transparency and clarity as to what requirements a cloud provider must comply with in order to process data for a particular sector, without losing the benefits of the cloud.

As earlier mentioned, the EC approved standard contractual clauses are not sufficient for all data processing constellations in the cloud. A possible area of legal research is to see how to ameliorate such deficiencies by expanding the clauses, and to what extent the proposed Common European Sales Law (CESL) could apply in the cloud. No less important for further legal research is the impact of the newly proposed Data Protection Regulation. How new rights such as the right to be forgotten and right to data portability will be implement in a cloud environment is yet to be known. Furthermore, the legal position of the cluster of middlemen or intermediaries in the cloud, such as cloud brokers needs to be reviewed in the future. The data controller-processor dichotomy of the present data protection law appears not fit properly into the cloud context.

4.1 Conclusion

In WP 7.2.1, we investigated the legal aspects of cloud computing specifically focusing on data protection, data security, intellectual property rights and green legislation relevant to the project. Having identified core data protection and security issues in cloud, we recommended a series of technical implementations in the various components of the OPTIMIS toolkit, such as data location restrictions, encryption, monitoring tools, facility to use the EC approved standard contractual clauses for international data transfer, etc. Furthermore, for the harmonization of the toolkit licenses, we performed a license check for all the components, and finally developed a legal guidance for those wishing to use the toolkit to be aware of data protection and compliance issues they may face. It is hoped that these measures will achieve the intention of this work package, which is to implement a level of privacy right from the design of the OPTIMIS toolkit.

\(^{114}\) http://www.cloudlegal.ccis.qmul.ac.uk/
Annex A. Cloud Legal Guidance for Data Protection Compliance

The power-balance between data controllers and data processors anticipated in the traditional data protection law may be difficult to apply in cloud computing scenarios. One thing that however remains unchanged is that data controllers who process data through a cloud service provider are not relieved of their legal obligation relating to data protection and security. It is therefore important to have a data protection impact assessment before deploying data to the cloud.

In view of the multiple scenarios in which cloud services could be used, this guide is generic in nature. Cloud computing is not a one-size-fits-all product, and in many cases, it could be tailored to fit the specific needs of an organization, for instance, in a private cloud. Therefore, an adaptation of this guidance to suit individual cases is appropriate. The OPTIMIS toolkit represents a Platform as a Service tool, available for both cloud service provider and infrastructure provider; it is left for the user of the toolkit to implement data protection policy using this guide as a reference point. The toolkit on its own has embedded certain mechanisms to assist in this process such as providing a monitoring tool, easy incorporation of the standard contractual clause and binding corporate rules. Restrictions can also be placed on the jurisdiction for the localization of data and other processes when using the toolkit. However, these should be complemented with other organizational and contractual measures.

While this guidance is aimed primarily at users of the OPTIMIS toolkit, it is also valuable to the general public and organizations using cloud services or considering moving to cloud services. For cloud service providers, it will show them what data protection issues their customers may need to deal with, and help them in adjusting their policies in order to assist their customers to stay compliant. Generally, the following issues should be considered when using cloud services:

To comply with key data protection considerations, cloud users should consider the following:

1. It is important to carry out an appropriate assessment of the outsourcing structure from a personal data protection perspective. A data protection impact assessment will reveal the extent of risk involved in the transaction and give room for implementing mitigation actions before starting the data processing.

2. Clearly identify what roles the parties involved in the cloud transaction will play. This in essence will show who the data controller, processor and sub-processor will be for compliance purposes. Data controllers who deploy data to the cloud are not relieved of their legal obligations relating to data protection and security. Therefore, they should implement necessary restrictions such as data localization before deployment, as well as have a monitoring tool to check whether the services are carried out in compliance with their instruction and restriction.

3. Identifying the roles of the parties will equally have an impact on the security aspects of the data processing. Cloud customers should understand the security framework of the services they want to use. This is important so that they will know their responsibilities in the data management as this may differ depending on the service – PaaS, SaaS, IaaS.

4. Clearly identify which countries personal data will be flow during service provisioning. This will assist the data controllers to implement appropriate safeguards such as using approved standard contractual clauses, safe harbor or binding corporate rules for international data transfer.
5. Ensure that appropriate mechanisms are put in place in order to be able to monitor the activities of the cloud provider. This will ensure compliance with data protection requirements.

6. Always check whether the cloud provider has received security, privacy and other certification from an independent third party, as it may not be possible for every cloud customer to carry out an individual audit.

7. Understand the nature of the cloud contract used for the data processing. The following clauses should be properly checked and the following questions answered:\[115\]

**i. Limitation of liability clauses:**

Who is liable for data protection violations such as data loss in the course of the service provisioning, and is this liability limited to a specific amount or entirely excluded? What possibilities are foreseen in enforcing the providers’ contractual obligations (e.g., penalty and indemnity clauses).

**ii. Unilateral modification of contract:**

Does the contract allow one party to change or amend the service unilaterally, and if so, is there an obligation to notify the other party before the modifications become effective? Is there an explicit right to terminate the contract if the modification is not accepted?

**iii. Use of sub-contractors/sub-processor:**

Are internal or external sub-processors used to offer the service and are they listed in the contract? Is there an obligation to bind all sub-processors with same obligations existing between customer and provider?

**iv. Location of data:**

Does the provider reveal all possible locations of the data centers used in processing, and, to increase the level of data protection, can you select which locations to store/process data?

**v. International transfer of data:**

Does the contract describe under which circumstances data would be transferred to third countries, and will adequate measures be provided for the transfer such as the use of standard contractual clauses, BCR, Safe Harbor, and so forth?

**vi. Security responsibilities and data breach notice:**

Does the contract fully describe data security measures and responsibilities between the parties such as backups, access control, encryption etc., and does the provider have a clear obligation to notify the customer of data breaches?

vii. **Transition at the end/termination of service:**
Is there a right to get back data in a usable format when the services are no longer needed or are terminated for any reason, without unnecessary restrictions?

viii. **Data retention and deletion clause:**
Is there a retention period for the provider to keep the data for the customer, and is the provider obligated to delete all personal data (including backups, Virtual Machine (VM) images, etc) after termination?

ix. **Law enforcement access to data:**
Does the contract handle transfer and access to stored data requested by foreign governmental agencies, and is the provider obligated to notify the customer about such a request?

x. **Rights of data subjects:**
Is the provider under obligation to support the customer with his duties as a controller to ensure and enforce data subjects’ rights?

xi. **Applicable jurisdiction:**
In the case of a dispute, which law applies and which court will have jurisdiction?

xii. **Providers’ Access to data:**
Who can access the stored data and for which reasons, and does the contract contain a confidentiality clause, which will apply for all employees and sub-processors?

8. Clearly state the intellectual property rights in the contract, indicating who owns the deployed data and the metadata accruing from the services and how they should be used.

9. The data controller should inquire whether other sub-processors would be used for the cloud services. Where this is the case, the data controller should know their location, and any subsequent changes should be brought to the data controller’s attention.

10. It is recommended that cloud service providers use, in addition to SLAs, PLAs as a measure of assessing their compliance with EU data protection framework. A sample of a PLA has been developed by the CSA and available on their website.¹¹⁶

## Annex B. List of Sampled Cloud Providers

Table 2. Sampled Cloud providers

<table>
<thead>
<tr>
<th>Provider offer</th>
<th>Documents</th>
<th>Link</th>
<th>Last date accessed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimension Data</td>
<td>Terms of service, SLA</td>
<td><a href="http://eucloud.dimensiondata.com/Legal/TOS">http://eucloud.dimensiondata.com/Legal/TOS</a></td>
<td>17.04.2013</td>
</tr>
<tr>
<td></td>
<td>Service Description</td>
<td><a href="http://eucloud.dimensiondata.com/Legal/Service-Level-Agreement">http://eucloud.dimensiondata.com/Legal/Service-Level-Agreement</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://virtualization.dimensiondata.com/Services/CloudServices/CaaS/Public/ServiceDescription/Pages/Home.aspx">http://virtualization.dimensiondata.com/Services/CloudServices/CaaS/Public/ServiceDescription/Pages/Home.aspx</a></td>
<td></td>
</tr>
<tr>
<td>Cloud Sigma</td>
<td>Terms of Service (ToS), AUP, Privacy policy, SLA</td>
<td><a href="http://virtualization.cloudsigma.com/en/platform-details/legal?t=0">http://virtualization.cloudsigma.com/en/platform-details/legal?t=0</a></td>
<td>17.04.2013</td>
</tr>
<tr>
<td>Company</td>
<td>Terms</td>
<td>URL</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>GoGrid</td>
<td>Terms of Service</td>
<td><a href="http://virtualization.gogrid.com/legal/terms-service">http://virtualization.gogrid.com/legal/terms-service</a></td>
<td>17.04.2013</td>
</tr>
</tbody>
</table>
Annex C. References

Books and Articles

Accenture

Alecu, Felician
Cloud Computing Solutions, Economy Informatics, Vol. 9, No. 1, 2009, pp. 105-111

Baaliga, Jayant et al

Becker, Philipp and Nikolaeva, Julia

Borchers, Detlef and Kuri, Jürgen

Bose, Sumit et al.

Bradshaw, Simon, Millard, Christopher and Walden, Ian

Calloway, Timothy J.

Cloud Industry Forum

Cloud Standards Customer Council

CSA Privacy Level Agreement Working Group

Fischl, Thomas and Weimer, Katharina A.
Forgó, Nikolaus, Barnitzke, Benno, Corrales, Marcelo


Garg, Saurabh Kumar and Buyya, Rajkumar


Gartner


Geyer, Andrew and McLellan, Melinda


Gilbert, Francoise


Gilbert, Francoise


Google


Hon, W. Kuan, Millard, Christopher and Walden, Ian


IBM


Kousiouris, George; Vafiadis, George and Corrales, Marcelo


Legal iQ


Maxwell, Winston and Wolf, Christopher

A Hogan Lovells White Paper, A Global Reality: Governmental Access to Data in the Cloud, A comparative analysis of ten international jurisdictions – Governmental access to data stored in the Cloud – including cross-border access – exists in
D7.2.1.4 Cloud Legal Guidelines


NIST


Out-law.com by Pinsent Masons


Ottenheimer, David


Patel, Pankesh; Ranabahu, Ajith and Sheth, Amit


Pell, Stephanie K.

Systematic government access to private-sector data in the United States, 2012, International Data Privacy Law Volume 2, No. 4

Phipps, Simon


Pittmans


Reavis, Jim


Reed, Chris


Svantesson, Dan Jerker B.


Tung, Liam


Vincent, Mark, Hart, Nick and Morton, Kate


Walden, Ian

Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, 2011, available at:
Whittaker, Zack

Microsoft admits Patriot Act can access EU-based cloud data, 2011, available at:

Winkler, Vic J. R.


Other Documents


European Commission COM(2012) 11 final, Proposal for a Regulation of the European


Italian Data Protection Authority, How to Protect Your Data Without Falling From a Cloud, 2012, available at: http://www.garanteprivacy.it/documents/10160/2052659/CLOUD+COMPUTING+%E2%80%93+PROTECT+YOUR+DATA+WITHOUT+FALLING+FROM+A+CLOUD.pdf


Annex D. License conditions

This is a public deliverable that is provided to the community under the license Attribution-NoDerivs 2.5 defined by creative commons http://www.creativecommons.org

This license allows you to

to copy, distribute, display, and perform the work

to make commercial use of the work

Under the following conditions:

Attribution. You must attribute the work by indicating that this work originated from the IST-OPTIMIS project and has been partially funded by the European Commission under contract number IST-257115

No Derivative Works. You may not alter, transform, or build upon this work without explicit permission of the consortium

For any reuse or distribution, you must make clear to others the license terms of this work.

Any of these conditions can be waived if you get permission from the copyright holder.

This is a human-readable summary of the Legal Code below:

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE (“CCPL” OR “LICENSE”). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

"Collective Work" means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.

"Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

"Licensor" means all partners of the OPTIMIS consortium that have participated in the production of this text

"Original Author" means the individual or entity who created the Work.

"Work" means the copyrightable work of authorship offered under the terms of this License.

"You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

2. Fair Use Rights. Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

- to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;
- to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works.

For the avoidance of doubt, where the work is a musical composition:

Performance Royalties Under Blanket Licenses. Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g. webcast) of the Work.

Mechanical Rights and Statutory Royalties. Licensor waives the exclusive right to collect, whether individually or via a music rights society or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and
distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

Webcasting Rights and Statutory Royalties. For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Derivative Works. All rights not expressly granted by Licensor are hereby reserved.

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients’ exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any credit as required by clause 4(b), as requested.

If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or Collective Works, You must keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or (ii) if the Original Author and/or Licensor designate another party or parties (e.g. a sponsor institute, publishing entity, journal) for attribution in Licensors copyright notice, terms of service or by other reasonable means, the name of such party or parties; the title of the Work if supplied; and to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. Representations, Warranties and Disclaimer. UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE MATERIALS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

Each time You distribute or publicly digitally perform the Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

© OPTIMIS Consortium