

D1.2.3

Cloud Computing – Solutions and Enablers

Project number:	257243
Project acronym:	TClouds
Project title:	Trustworthy Clouds - Privacy and Resilience for Internet-scale Critical Infrastructure
Start date of the project:	1 st October, 2010
Duration:	36 months
Programme:	FP7 IP

Deliverable type:	Report
Deliverable reference number:	ICT-257243 / D1.2.3/ 1.0
Activity and Work package contributing to the deliverable:	Activity 1 / WP 1.2
Due date:	September 2012 – M24
Actual submission date:	19 th October, 2012

Responsible organisation:	ULD
Editor:	Ninja Marnau
Dissemination level:	Public
Revision:	1.0

Abstract:	This deliverable aims at identifying solutions and enablers to lawfully make use of cloud computing. To adequately protect personal data while using cloud computing, the risks need to be mitigated on three levels: politically, contractually, and technically. We describe measures and approaches on the three levels that aim at enabling cloud computing and enhancing privacy and security.
Keywords:	Data Protection, Privacy Enhancing Technologies, Privacy Impact Assessment, Certification Frameworks

Editor

Ninja Marnau (ULD)

Contributors

Ninja Marnau (ULD)

Meiko Jensen (ULD)

Eva Schlehahn (ULD)

Ricardo Morte Ferrer (ULD)

Disclaimer

This work was partially supported by the European Commission through the FP7-ICT program under project TClouds, number 257243.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose.

The user thereof uses the information at its sole risk and liability. The opinions expressed in this deliverable are those of the authors. They do not necessarily represent the views of all TClouds partners.

Executive Summary

In this deliverable we evaluate possible enablers for cloud computing with regard to the European legal framework. Enablers from several disciplines are evaluated to provide a comprehensive overview, since only in combination sufficient security and data protection can be obtained. We discuss legal policies, contractual, certification and technical enablers.

First, we start by showing in Chapter 2 the gaps and shortcomings in the current legal framework and make suggestions how to address these.

In Chapter 3 we provide an outlook on the future development in the EU. We describe the proposed Data Protection Regulation and the European Cloud Strategy, considering in which way these may prove to be cloud-enabling.

Continuing with specific contractual measures enabling cloud computing in Chapter 4, we list contractual means as guidelines for a cloud customer to negotiate a cloud service contract or evaluate the offered SLAs. Additionally, Processor BCR are reviewed and their impact on CSPs is highlighted.

Chapter 5 of this document investigates technical solutions to recurring problems of cloud security. A major part of this chapter covers common certification and assessment frameworks for cloud provider security conditions. Specifically, the major certification and assessment frameworks of ENISA, BSI, Cloud Security Alliance, and EuroCloud are investigated and evaluated in terms of capabilities and suitability for legal assessments of cloud service providers. The second part of Chapter 5 analyses a set of common technical means to improve cloud security, ranging from anonymization over use of cryptography to architectural and organizational aspects of the cloud environment, and the last part of this chapter focuses on specific technical enablers invented within the TClouds project.

Contents

Chapter 1 Introduction	1
1.1 TClouds – Trustworthy Clouds.....	1
1.2 Activity 1 – Legal and Business Foundations for Cross-Border Computing	1
1.3 Work Package 1.2 – Legal Implications and Impact of Cross-Border Cloud Implementations.....	2
1.4 Deliverable 1.2.3 Cloud Computing – Solutions and Enablers.....	2
1.4.1 Structure	2
1.4.2 Deviation from Work Plan.....	2
1.4.3 Relation to other Deliverables	3
Chapter 2 Analysis of Gaps in the Current Legal Framework	4
2.1 Revision of the EU Data Protection Directive.....	4
2.1.1 Removing Jurisdiction Uncertainties	6
2.1.2 Sharpening the Definition of Personal Data.....	6
2.1.3 Clearer Definition and Requirements on Consent	7
2.1.4 Establishing the Principles of Accountability, Privacy by Design (PbD), and Security by Design (SbD)	8
2.1.5 Harmonisation and Consistency of Data Protection Legislation in General	10
2.1.6 Harmonisation regarding Data Security Measures	11
2.1.7 Empowering the DPAs	11
2.1.8 Harmonising Processing Notification Procedures.....	12
2.1.9 Empowering Data Subjects and Improving Enforcement.....	12
2.1.10 Redesign of the Adequacy Process	13
2.1.11 Additional Discussion Points	14
2.1.12 Modification of the EU Standard Contractual Clauses	14
2.1.13 Further Development of BCR	16
2.2 Conclusion and Outlook to Supplementary Means	17
Chapter 3 Outlook on Future Development.....	18
3.1 Proposed Data Protection Regulation.....	18
3.2 European Cloud Computing Strategy	19
Chapter 4 Contractual Enablers	22
4.1 Individual Contracts and SLA.....	23
4.1.1 Scope of the Contract	24
4.1.2 Data Protection and Data Security Topics.....	24

4.1.2.1	<i>Involved Data and Purpose Specification</i>	24
4.1.2.2	<i>Location of Facilities</i>	25
4.1.2.3	<i>Transborder Transfer of Data</i>	25
4.1.2.4	<i>Confidentiality of the CSP</i>	25
4.1.2.5	<i>Notification of Governmental Access</i>	26
4.1.2.6	<i>Subcontractors</i>	26
4.1.2.7	<i>Control and Intervenability</i>	27
4.1.2.8	<i>Change Notification</i>	27
4.1.2.9	<i>Breach Notification</i>	27
4.1.2.10	<i>Deletion</i>	27
4.1.2.11	<i>Decency Checks</i>	28
4.1.3	Technical Security Measures	29
4.1.3.1	<i>Isolation</i>	29
4.1.3.2	<i>Monitoring</i>	29
4.1.3.3	<i>Logging</i>	29
4.1.3.4	<i>Encryption</i>	30
4.1.3.5	<i>Availability</i>	30
4.1.4	General Contractual Topics	31
4.1.4.1	<i>Disaster Recovery and back-ups</i>	31
4.1.4.2	<i>Business Continuity</i>	31
4.1.4.3	<i>Cancellation</i>	31
4.1.4.4	<i>Portability / Vendor lock-in</i>	31
4.1.4.5	<i>Contractual Penalties</i>	31
4.1.4.6	<i>Liability</i>	31
4.1.4.7	<i>Place of Jurisdiction</i>	31
4.1.4.8	<i>Forensics Cooperation</i>	32
4.1.4.9	<i>Intellectual Property</i>	32
4.1.4.10	<i>Licensing</i>	32
4.2	Processor BCR	32
4.2.1	<i>Public Availability</i>	33
4.2.2	<i>Liability</i>	33
4.2.3	<i>Commitment to cooperation</i>	33
4.2.4	<i>Transparency on subcontractors</i>	34
Chapter 5	Technical Solutions an Enablers	35
5.1	Cloud Provider Certification Frameworks	38
5.1.1	BSI Baseline Protection	38
5.1.1.1	<i>Baseline Protection and ISO/IEC 27001</i>	38
5.1.1.2	<i>Security Recommendations for Cloud Computing Providers</i>	39
5.1.2	ENISA Procure Secure	40
5.1.2.1	<i>Service Availability</i>	42
5.1.2.1.1	<i>Technical Description</i>	42

5.1.2.1.2	Customer Risk Assessment	43
5.1.2.1.3	Contractual Considerations	44
5.1.2.1.4	Technical issues of monitoring and assessment.....	44
5.1.2.1.4.1	<i>Incident Response</i>	44
5.1.2.1.5	Technical Description	44
5.1.2.1.6	Customer Risk Assessment	45
5.1.2.1.7	Contractual Considerations	45
5.1.2.1.8	Technical issues of monitoring and assessment.....	45
5.1.2.2	<i>Service Elasticity and Load Tolerance</i>	46
5.1.2.2.1	Technical Description	46
5.1.2.2.2	Customer Risk Assessment	46
5.1.2.2.3	Contractual Considerations	47
5.1.2.2.4	Technical issues of monitoring and assessment.....	47
5.1.2.3	<i>Data Lifecycle Management</i>	47
5.1.2.3.1	Technical Description	47
5.1.2.3.2	Customer Risk Assessment	48
5.1.2.3.3	Contractual Considerations	48
5.1.2.3.4	Technical issues of monitoring and assessment.....	48
5.1.2.4	<i>Technical Compliance and Vulnerability Management</i>	49
5.1.2.4.1	Technical Description	49
5.1.2.4.2	Technical issues of monitoring and assessment.....	49
5.1.2.5	<i>Change Management</i>	50
5.1.2.5.1	Technical Description	50
5.1.2.5.2	Customer Risk Assessment	50
5.1.2.5.3	Contractual Considerations	50
5.1.2.5.4	Technical issues of monitoring and assessment.....	50
5.1.2.6	<i>Data Isolation</i>	51
5.1.2.6.1	Technical Description	51
5.1.2.6.2	Customer Risk Assessment	51
5.1.2.6.3	Contractual Considerations	51
5.1.2.6.4	Technical issues of monitoring and assessment.....	52
5.1.2.7	<i>Log Management and Forensics</i>	52
5.1.2.7.1	Technical Description	52
5.1.2.7.2	Customer Risk Assessment	52
5.1.2.7.3	Contractual Considerations	53
5.1.2.7.4	Technical issues of monitoring and assessment.....	53
5.1.2.8	<i>Evaluation</i>	53
5.1.3	CSA STAR, CAIQ, and the Cloud Controls Matrix.....	56
5.1.3.1	<i>Cloud Controls Matrix (CCM)</i>	56
5.1.3.2	<i>Consensus Assessments Initiative Questionnaire (CAIQ)</i>	57
5.1.3.3	<i>The CSA Security, Trust, and Assurance Registry (CSA STAR)</i>	58
5.1.4	EuroCloud and the SaaS Star Audit	59
5.2	Privacy-Enhancing Approaches for Commodity Clouds.....	60
5.2.1	Anonymization and Pseudonymization.....	60
5.2.2	Encryption and Digital Signatures	61

5.2.3	Usage of Multiple Cloud Environments.....	62
5.2.3.1	<i>Global Legal Considerations on Utilizing Multiple Cloud Providers</i>	63
5.2.3.2	<i>Knowledge Splitting Approaches</i>	64
5.2.3.2.1	Plain Redundancy („Replication of Data/Application“)	64
5.2.3.2.2	Data Splitting	65
5.2.3.2.3	Process Splitting	67
5.2.3.3	<i>Hybrid Clouds, and InterClouds</i>	68
5.2.3.4	<i>Homomorphic Encryption</i>	69
5.2.3.5	<i>Secure Multi-Party Computation Clouds</i>	71
5.3	Specific Enablers from the TClouds Architecture.....	72
5.3.1	TPM Virtualization.....	72
5.3.1.1	<i>Fundamentals of TPM</i>	72
5.3.1.2	<i>TPM and Clouds: the Multi-Tenancy Problem</i>	74
5.3.1.3	<i>The TClouds Approach to TPM Virtualization</i>	74
5.3.2	The TwinClouds Approach	75
5.3.3	The DepSky Approach	77
Chapter 6	List of Abbreviations	78
Chapter 7	Bibliography	80
7.1	Literature.....	80
7.2	Legislation.....	85
7.3	Official statements & opinions on EU and national level	85
7.3.1	European Commission.....	86
7.3.2	Other EU bodies	86
7.3.3	Article 29 Data Protection Working Party	87
7.3.4	National Level	88

List of Figures

Figure 1: WP1.2 Interdependencies	3
Figure 2 Cloud computing specific risks	22
Figure 3: Replication of data by using multiple clouds	65
Figure 4: Data splitting approach using two clouds	66
Figure 5: Process splitting by using multiple clouds	67
Figure 6: Intercloud example - Using multiple clouds to interact with each other for one process	69
Figure 7: Homomorphic Encryption using one single cloud	70
Figure 8: Secure Multi-Party Computation using multiple clouds	71

List of Tables

Table 1: Legal Responsibilities	23
Table 2: Overview of evaluated standards and guidelines	35
Table 3: Overview of addressed key issues	36
Table 4: List of abbreviations	78

Chapter 1

Introduction

1.1 TClouds – Trustworthy Clouds

TClouds aims to develop trustworthy Internet-scale cloud services, providing computing, network, and storage resources over the Internet. Existing cloud computing services are today generally not trusted for running critical infrastructure, which may range from business-critical tasks of large companies to mission-critical tasks for the society as a whole. The latter includes water, electricity, fuel, and food supply chains. TClouds focuses on power grids and electricity management and on patient-centric health-care systems as its main applications.

The TClouds project identifies and addresses legal implications and business opportunities of using infrastructure clouds, assesses security, privacy, and resilience aspects of cloud computing and contributes to building a regulatory framework enabling resilient and privacy-enhanced cloud infrastructure.

The main body of work in TClouds defines an architecture and prototype systems for securing infrastructure clouds, by providing security enhancements that can be deployed on top of commodity infrastructure clouds (as a cloud-of-clouds) and by assessing the resilience, privacy, and security extensions of existing clouds.

Furthermore, TClouds provides resilient middleware for adaptive security using a cloud-of-clouds, which is not dependent on any single cloud provider. This feature of the TClouds platform will provide tolerance and adaptability to mitigate security incidents and unstable operating conditions for a range of applications running on a cloud-of-clouds.

1.2 Activity 1 – Legal and Business Foundations for Cross-Border Computing

The Scope of Activity 1 is to identify requirements and boundaries for cloud computing. The Activity aims at providing a guidance framework to address both legal requirements and business interests in cross-border infrastructure clouds.

Based on the expertise and input from users and stakeholders, the activity researches relevant interests, drivers and obstacles for the use of cloud computing services for privacy-sensitive and business-critical applications – with a focus on the implication of cross-border cloud deployment.

Furthermore, an analysis of the European legal framework for data protection and data security will identify the regulatory foundation for cloud computing and lead to an investigation of its privacy impact.

The Activity addresses the business impact of cloud computing as well as the accompanying privacy and security concerns. Requirements derived from this tense relationship of business benefit and regulatory boundaries will be mapped to organisational, contractual and technical measures and enablers.

1.3 Work Package 1.2 – Legal Implications and Impact of Cross-Border Cloud Implementations

The objective of WP1.2 is to provide and define legal requirements for cloud computing in cross-border scenarios. Different legislation and jurisdiction on privacy- and IT-related issues of cloud computing will be analyzed. The analysis will enable us to provide solutions and additional measures for cross-border cloud scenarios. Furthermore, the privacy impact of cross-border clouds using well-known and standardized methods will be analyzed.

1.4 Deliverable 1.2.3 Cloud Computing – Solutions and Enablers

This deliverable aims at identifying contractual and technical solutions and enablers to lawfully make use of cloud computing. To address the legal requirements identified in D1.2.2 and to adequately protect personal data while using cloud computing, the risks need to be mitigated on three levels:

- Legal policies
- Contractually
- Technically

We describe measures and approaches on the three levels that aim at enabling lawful cloud computing and enhancing privacy and security.

1.4.1 Structure

The deliverable is structured in four major parts. It starts by addressing gaps and frictions in the current legal framework of the Data Protection Directive 95/46/EC by making suggestions for a revision of this legal framework. Furthermore, the proposed EU Data Protection Regulation is considered with regard to its impact on cloud computing.

To counter the legal uncertainties and requirements we identified in D1.2.2 “Cloud Computing: Legal Analysis” we take a look at guidelines and frameworks from the three levels of mitigation mentioned above. We start with political enablers such as the European Cloud Strategy and then continue with contractual enablers including a comprehensive list of contractual topics and rules to adhere to when negotiating cloud computing contracts.

We also consider several technical enablers, including recognized certification frameworks and auspicious academic approaches to enhance secure cloud computing using one or multiple clouds.

1.4.2 Deviation from Work Plan

This document extends the work plan from the Annex1 (DoW) for Task 1.2.3. Plan for Task 1.2.3 was to investigate technical compliance requirements with legal impact, in particular Sarbanes Oxley, CoBIT, ITIL, ISO27001, IT Baseline Protection (“BSI Grundschutz”) and other standards of good/best-practice in IT operation and security. Our research indicated that some of these mentioned standards of good practice, namely Sarbanes Oxley, CoBIT, and ITIL, hardly relate and integrate with the general architecture of cloud computing ecosystems. We therefore considered other standards of good practice especially tailored for cloud computing providers and users by ENISA and EuroCloud.

Additionally, we looked at academic approaches to enhance security in cloud computing and provide legal consideration with regard to the European law.

1.4.3 Relation to other Deliverables

This Deliverable is based on the comprehensive analysis of the European legal framework for data protection and data security published in D1.2.2. On this basis D1.2.3 identifies legal shortcomings and possible approaches to bridge these shortcomings. These organisational, contractual and technical solutions and enablers aim at fuelling and contributing to the international discussion about legal policies, proposed changes to the legal framework with regard to cloud computing and best practices. The research and results that contributed to this deliverable have been put forward to a number of legal policy committees and have influenced relevant international and national documents such as the German Guidelines for Cloud Computing of the Working Groups Technology and Media of the Conference of German DPAs¹ and the Cloud Opinion of the Article 29 Working Party². Please refer to D4.1.2 for further information.

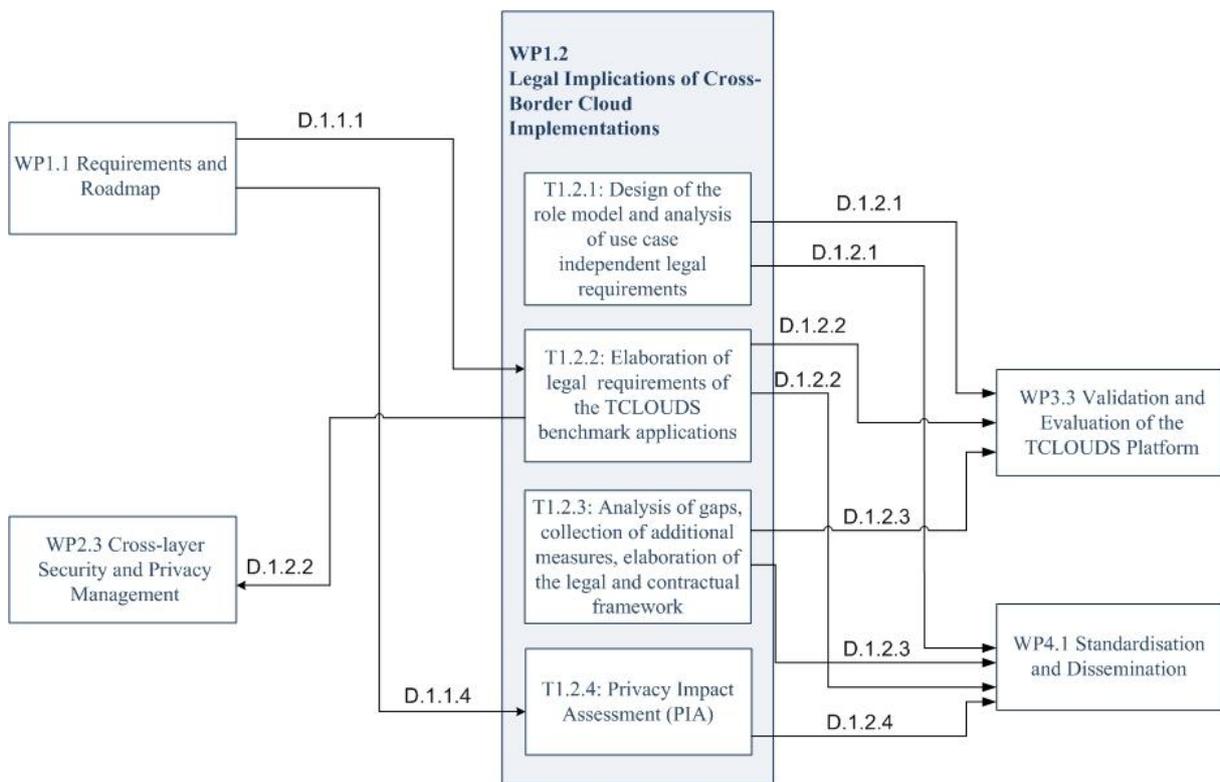


Figure 1: WP1.2 Interdependencies

¹ Orientierungshilfe – Cloud Computing http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

² Opinion 05/2012 on Cloud Computing http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Chapter 2

Analysis of Gaps in the Current Legal Framework

The increasing use of new electronic communication forms and technologies, such as Web 2.0 or cloud computing, come along with a number of issues related to the adequate protection of personal data in these contexts. The two key objectives of the European Data Protection Directive 95/46/EC currently in force, the protection the personal data of individuals while enabling a free flow of data in the internal market, are core principles that are still valid nowadays. To achieve their full effect however, they necessitate a comprehensive evaluation and revision of the current European Data Protection Directive to adjust this legal framework to the societal and technological developments of the modern world. In our deliverable D1.2.2 (“Cloud Computing: Legal Analysis”), we analysed that particularly in the light of new technologies, such as cloud computing, the Data Protection Directive has shown several shortcomings. This specifically, but not conclusively, applies to the distinction between data controllers and processors, the question of applicable law and the enforcement of data protection requirements. Especially for cases of cross-border data transfers and the correlating legal issues, EU Standard Contractual Clauses and Binding Corporate Rules may be useful tools to overcome those hurdles. Nevertheless, they still need further development to meet the challenges of the latest technological developments and enable full exploitation of new business models in the ICT field in compliance with European data protection requirements. This document will address possible improvements concerning the protection of personal data by additional measures. Thereby, it will focus on the organisational, contractual and technical aspects to achieve such improvements.

2.1 Revision of the EU Data Protection Directive

The European Data Protection Directive is currently undergoing revision by the European Commission. In force since 1995, the generally technology-neutral nature of the Directive still confronts users and providers of new technologies with a number of uncertainties and obstacles in respect to the treatment of personal data as well as the effective implementation and enforcement of its protection. The potential multitude of parties involvedr cloud computing contexts and the immense quantity and quality of data that is shared via social networks significantly increases the risks personal data is subjected to nowadays.³

On these grounds, the European Commission focuses on a number of proposed changes for its ongoing revision of the European data protection framework, which may be reduced to four key objectives:

³ Article 29 Working Party, WP 168, *The Future of Privacy – Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, adopted on 01 December 2009, p. 12

- Overhaul of the data controller's duties and obligations concept
- Raising the individual's awareness and comprehension in respect to privacy issues
- Strengthening the individuals' rights
- Facilitating the free flow of information in the internal and cross-border market to maintain and foster the economic strength and growth of the EU, its companies and citizens⁴

From the industry's point of view, the European Data Protection Directive does not need specific regulations tailored for specific processing contexts, such as cloud computing. The core principles of data protection in the Directive are seen as universally applicable. However, some amendments and improvements would still be needed. Businesses complain that the legal framework imposes considerable hurdles that hinder European companies to freely exercise their businesses and put them at competitive disadvantage in comparison to companies of third countries. In respect to the revision work of the European Commission, business associations as well as single companies expressed demand for a lessening of administrative burdens, better support of a free flow of data across countries and a comprehensive and integrative system to ensure the flourishing of the European market.⁵ Conflicting protection goals also play a role for businesses, such as the protection of own business secrets. This being said, companies don't want to disclose details of their own security and data protection measures, which may be detrimental to the empowering of user's and data subjects according to the objectives of the EU Data Protection Directive. Moreover, businesses suggest for industry-led approaches to standardisation and interoperability.⁶ In regard to legal responsibility, businesses propose contractual solutions as preferable to regulate liabilities, especially in complex layers of involved parties and contracts.⁷

⁴ See Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM (2010) 609 final of 4 November 2010, *A comprehensive approach on personal data protection in the European Union*, p. 5 ff; See also:

Response to the Call for Evidence on the Current Data Protection Legislative Framework carried out by the Ministry of Justice UK; Call for Evidence on the Current Data Protection Legislative Framework <http://www.justice.gov.uk/consultations/docs/dpa-call-evidence-response-paper-28-01-11a.pdf>

⁵ The European Telecommunications Network Operator's Association (ETNO) called this the "same level playing field" in regard to European companies compared to companies from third countries; cf. the ETNO Position Paper published in January 2011: *Reflection Document on the EU Public Consultation on the Communication on a comprehensive approach on personal data protection in the European Union*, p. 2ff.

⁶ See ETNO Position Paper of August 2011: *Reflection Document replying to the public consultation on Cloud Computing*, p. 11ff.

⁷ Cf. ETNO Position Paper of January 2011: *Reflection Document on the EU Public Consultation on the Communication on a comprehensive approach on personal data protection in the European Union*, p. 9ff.

2.1.1 Removing Jurisdiction Uncertainties

A critical issue is the question of the applicability of the EU member states' national data protection laws under the umbrella of the EU Data Protection Directive 95/46/EC especially in cases of cross-border data transfers. As we already analysed in our Deliverable D1.2.2, the EU Directive manifests rough provisions under which the applicable law can be determined. These provisions are

1. the activities of an establishment of the controller in one of the EU member countries⁸,
2. the applicableness of national law by virtue of international public law⁹ or
3. the use of automated or non-automated equipment for data processing, located in an EU member country, except for purposes of mere data transit.¹⁰

The most crucial provision of these three is the establishment of the controller as a means to determine the applicability of national EU member state law. This provision however, causes problems, for instance, in cases of a third-country located cloud service vendor without any facilities within the EU area that offers its services to European citizens. In such cases, neither European data protection law is applicable at all (provision 1), nor the protection of personal data according to European standards is ensured (provisions 2 & 3). Also, the relationship of the European member states' national data protection laws to each other is unclear in situations such as the vendor having several facilities in different EU Member States.¹¹ Hence, a clearer statement of the European Data Protection Directive in respect to its applicability and the direct effect of the national law within its scope would remove much legal uncertainties. Such a statement could involve an additional criterion of the affection of EU citizens to grant adequate protection of their personal data once they make use of international services of non-EU vendors.

2.1.2 Sharpening the Definition of Personal Data

The European Data Protection Directive grants protection to individual's personal data. According to Article 2 (a) of the Directive, "*'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;*" This definition, though, is often deemed unsatisfactory due to uncertainties, when data may be relatable to an identified or identifiable individual. For instance, data like information about buildings (in relation to their owners), energy meter numbers, and energy consumption. Moreover, the decision if anonymized or encrypted data must be considered as being personal is also left open to widely differing interpretation of the Directive's provisions. In respect to sensitive personal data, the inclusion of biometric data into the scope of the definition may be discussable, depending on the context of the processing.¹² In respect to provisioned exceptions for the obtainment of consent, restricting

⁸ Article 4 (1) lit. a) of the Directive.

⁹ Article 4 (1) lit. b) of the Directive.

¹⁰ Article 4 (1) lit. c) of the Directive.

¹¹ Article 29 Working Party, WP 168 p. 9.

¹² See Response to the Call for Evidence on the Current Data Protection Legislative Framework carried out by the Ministry of Justice UK, p. 7 f.

those in cases of processing statistical or scientific purposes may be discussable. Furthermore there is an obvious conflict between the objectives of personal data protection on the one hand and the freedom of speech related to the processing of data for journalistic purposes. In this regard, a well-grounded and adequate balance must be maintained. Moreover, the scope of the European Data Protection Directive does not extend over personal data processing in a purely personal context or household activities.¹³ This restriction however, may cause the loss of the data protection law once a person reaps the benefits of online services for his own domestic purposes, only using his own personal data, like in cases of cloud computing usage. While not in all cases of individuals using cloud computing, the impact of European data protection runs into blankness, the distinction of personal data processing being domestic or non-domestic use may still be quite relevant. Thus, the exceptions of purely personal or domestic use are limitations that undesirably deprive data subjects of much needed protection. Insofar, an extension of the EU Data Protection Directive's scope must be considered.¹⁴

2.1.3 Clearer Definition and Requirements on Consent

Uncertainties in respect to the provision of valid consent by the data subject to process his personal data show the need of a clearer definition within the European data protection framework. Article 2 (h) of the European Data Protection Directive 95/46/EC gives the following definition on consent:

"[The] data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

The Article 29 Working Party adopted a document in July 2011, providing some guidance on the definition of consent, giving tangible examples focusing on the vital elements of consent-giving situations, such as the meanings of "indication", "freely given", "specific", "unambiguous", "explicit" and "informed". In a second step, the document gives recommendations for the current revision of the Data Protection Directive, deriving from the analysis of these key elements. The recommendations entail the following points¹⁵:

- A need to sharpen the term "unambiguous" in such a fashion that the clear and unwavering agreement must be expressed through the consent notion;
- An explicit obligation for data controllers to provide evidence of given consent in consideration of supervision and accountability
- manifesting clear requirements on quality and accessibility of the information that forms the basis for the giving of the consent
- suggestions regarding minors and others lacking the legal capability of giving valid consent by themselves

¹³ Article 3 (2) Data Protection Directive..

¹⁴ Council of Europe project cybercrime p. 12 ff.; see also the speech held by the European Data Protection Supervisor Peter Hustinx at the Third European Cyber Security Awareness Day BSA, European Parliament on 13 April 2010 in Panel IV: Privacy and Cloud Computing: "Data Protection and Cloud Computing under EU law", p. 5 f.

¹⁵ Article 29 Working Party, WP187, *Opinion 15/2011 on the definition of consent*, adopted on 13 July 2011.

These recommendations encompass well-grounded arguments, capturing the essence of legal and practical issues regarding the giving of consent. Especially globally operating IT service providers, such as in the cloud computing industry, impose their more or less general terms of service and data protection policies upon their customers. Thereby they extensively exclude their own liabilities and veil their means to protect the personal data their customers entrust to them. Additionally, it is intolerable effort required of customers to constantly monitor and compare the ToS and privacy policies of their contract partners whether significant changes were made. This current factual situation of data subjects and service customers being subjected to the goodwill of such market power reveals an urgent need for more transparency as an adequate ground to give informed consent for the data processing activities. Thus, valid consent must necessitate lucidity and fairness in respect to the conditions under which consent is supposed to be given. A supporting aspect is the increase of citizen's awareness in regard to their individual data protection rights. Moreover, the forensic aspects of the consent notion are of importance for service providers while undergoing inspection by supervisory authorities and to meet their accountability requirements. Finally, gaps in legal capability for giving consent need harmonised and sufficient regulation to avoid the loss of control and adequate protection for concerned person's personal data.

2.1.4 Establishing the Principles of Accountability, Privacy by Design (PbD), and Security by Design (SbD)

Pursuant to the European Data Protection Directive 95/46/EC, the data controller is responsible for the lawfulness of the data processing in terms of data protection law. Hence, the distinction between data controller and data processor during any processing activities is crucial for the allocation of the legal responsibility. Once a service provider must be considered a data controller, his handling of accountability is of crucial importance for the trust into his business. In respect to the demand for reasonable execution of accountability, the Centre for Information Policy Leadership as Secretariat to the Galway Project defined five key elements that are decisive for its success. These elements are¹⁶:

- Organisation commitment to accountability and adoption of internal policies consistent with external criteria
- Mechanisms to put privacy policies into effect, including tools, training and education
- Systems for internal, ongoing oversight and assurance reviews and external verification
- Transparency and mechanisms for individual participation
- Means for remediation and external enforcement

¹⁶ See Centre for Information Policy Leadership as Secretariat to the Galway Project, Data Protection Accountability: The Essential Elements, A Document for Discussion, October 2009, p. 17 f. The Galway project is an initiative founded and fostered by Ireland's Office of the Data Protection Commissioner and co-sponsored by the OECD. It focuses on questions of responsibility and reliability in terms of data protection in respect to the rapidly progressing development and complexity of international data transfers.

The Article 29 Working Party also expressed that statutory establishment accountability would foster a much more intense protection of personal data pursuant to the principles of European data protection. Such regulation would make sure that data controllers strive more solicitously to use appropriate and effective measures in order to achieve compliance with the data protection requirements.¹⁷

Resolving data protection issues in new IT technologies, such as cloud computing can also be realised through the so-called Privacy by Design (PbD) approach. This approach is a concept first developed by the Canadian Information & Privacy Commissioner Dr. Ann Cavoukian in the 90's. It proposes that companies should develop, use and offer their services and the whole infrastructure around them as well as their related IT systems in a privacy-friendly manner from the very beginning. Cavoukian named a set of fundamental principles, which are as follows¹⁸:

- Enabling privacy should be proactive, not reactive; measures should be preventative not remedial
- Privacy should be implemented as the default setting
- Privacy should be embedded into the design of the service/product from the very beginning
- End-to-end security — full lifecycle protection of personal data from moment of collection to deletion after use
- Visibility and transparency should keep component parts and operations open to independent verification
- Respect for user privacy by offering knowledge and control

The National IT and Telecom Agency Copenhagen, Denmark, developed an alternate approach, called Security-by-Design (SbD). IT services shall consist of an architecture focusing on minimal data disclosure, providing maximal control for the user. Attribute-based credentials, virtual identities and transaction isolation should be used to hinder the relation to an identified or identifiable individual. Since cloud computing cases trigger an increasing need for trustworthy infrastructures, this approach shall also apply in such contexts.¹⁹

Such approaches like the principles of accountability, Privacy by Design and Security by Design also enable companies to meet the often stringent requirements of supervisory authorities for regulatory audits.

¹⁷ Article 29 Working Party, WP 173, Opinion 3/2010 on the principle of accountability, adopted on 13 July 2010 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf .

¹⁸ Ann Cavoukian, Information & Privacy Commissioner Ontario, Canada, Privacy by Design - The 7 Foundational Principles, originally published: August 2009, revised January 2011, <http://www.privacybydesign.ca>

¹⁹ The National IT and Telecom Agency Copenhagen, Denmark: New Digital Security Models - Discussion Paper, February 2011, p. 11 ff.

2.1.5 Harmonisation and Consistency of Data Protection Legislation in General

Throughout all potentially involved stakeholders, such as citizens, consumer protection organisations, industry, business associations and governmental bodies, the desire for a greater harmonisation of the European Data Protection Directive was voiced.²⁰ Especially the increasing use of new technologies that potentially involve cross-border data transfers, like cloud computing, reveal significant difficulties to accomplish compliance with the legal requirements of all of the individual EU member states. This poses major obstacles for both data controllers and data processors who find themselves subjected to a multitude of diverse regulations. Also, the enforcement of adequate data protection pursuant to the fundamental grounds of the Directive can prove exceedingly difficult in cases of such transnational data transfers.²¹

Initiatives towards binding international frameworks and the explicit requisition of international standardisation would facilitate such harmonisation and consistency. On this goal focuses for instance the Madrid Resolution²², which is a joint proposal on standards for privacy protection adopted by the International Conference of Data Protection and Privacy Commissioners in 2009.²³

The resolution drafts a global standard while summarising all potential approaches in this field, including principles, rights and obligations as a unified global basis for legal data protection. Moreover, international standards are demonstrated as useful to enable an adequate level of data protection worldwide.²⁴ However, while this resolution is a start, there is the need for further steps to facilitate an all-embracing realisation of European data protection principles. Also conceivable would be the statutory introduction of standardisation bodies to foster the development of such standards.

²⁰ See here for a list of statements on the public EU-consultation on the revision of the European data protection framework: http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm .

²¹ Google Official Enterprise Blog, entry of September 12, 2011, Supporting Europe's Efforts for More Cloud Adoption, http://googleenterprise.blogspot.com/2011/09/supporting-europes-efforts-for-more.html?utm_source=entblog&utm_medium=blog&utm_campaign=Feed%3A+OfficialGoogleEnterpriseBlog+%28Official+Google+Enterprise+Blog%29 ; Microsoft's Response to the Commission's Public Consultation on Cloud Computing 31 August 2011, <http://www.microsoft.eu/Portals/0/Document/Technology%20Policy/Microsoft%20response%20to%20EU%20cloud%20strategy%20public%20consultation.pdf> ;

European Telecommunications Network Operator's Association, Position Paper: ETNO Reflection Document replying to the public consultation on Cloud Computing, August 2011, <http://www.etno.eu/LinkClick.aspx?fileticket=11d%2fjaTJcS8%3d&tabid=2422> .

²² Madrid Resolution http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/InternationalDS/2009MadridResolution.pdf?__blob=publicationFile

²³ International Conference of Data Protection and Privacy Commissioners, held in Madrid on 5 November 2009, Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/InternationalDS/2009MadridResolution.pdf?__blob=publicationFile

²⁴ Article 29 Working Party, WP 168 p. 10.

2.1.6 Harmonisation regarding Data Security Measures

Art. 17 (1) 95/46 EC requires the data controller to *"implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access [...] and against all other unlawful forms of processing"*. The demands for appropriate measures are vague. They *"shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected"* but only in regard to *"the cost of their implementation"*. This vagueness leads to different requirements in the national implementations of the directive in the Member States. This is demonstrated by the implementation of the Data Retention Directive 2006/24/EC. The Data Retention Directive has a similar wording in regard to technical and organisational measures and does not specifically demand additional measures on top of the general measures of the Data Protection Directive. The Article 29 Working Party examined the compliance at national level of Telecom Providers and ISPs with the Data Retention Directive. The replies to the questionnaire and on-the-spot inspections showed a patchwork of implementing measures, with particular regard to the security measures in place.²⁵

This inhomogeneous implementation defies the aim of the Data Protection and Data Retention Directives to harmonise the security standard throughout Europe. For corporations with multinational assets in several European Member States it leads to additional costs to comply with all of these varying security requirements. It also prevents European residents from being afforded the same level of protection.²⁶

- strong access control to the retained data, via the definition of user responsibilities and profiles with different user privileges
- strong authentication for system access, based on dual authentication mechanisms (i.e. password + biometrics, or password + token), to ensure physical presence of the person in charge of processing traffic data
- detailed tracking of accesses and processing operations by way of log retention, via logs recording at least user identity, access time, file accessed
- deployment of log management solutions to ensure log integrity by means of encryption technology or measures that provide equivalent protection
- logical separation from other systems processing traffic data for commercial purposes
- such additional measures as may be necessary to ensure confidentiality of data
- security certification programmes
- enabling DPAs to carry out audits or making audits available to DPAs

2.1.7 Empowering the DPAs

The European DPAs are essential to safeguard the compliance and lawfulness of processing of personal data. To sufficiently fulfil this task it is necessary to strengthen the supervisory

²⁵ see Article 29 Working Party, WP 172, Annex 1, Columns P and Q
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_annex_en.pdf .

²⁶ Article 29 Working Party, WP 172, p. 14.

role of the national DPAs. The specific responsibilities and authorities of the DPAs vary among the Member States.

To verify and enforce the compliance of processing activities on personal data the national DPAs must be granted supplementary investigative powers. They must be enabled to perform unannounced on-sight inspections on the assets of the data controllers and processors. Furthermore, they must be enabled to issue a cease-and-desist letter in case of illegal processing activities. This is not the case in all member states. In addition, the possibilities of administrative sanctions should be harmonised in Europe. The maximum amount of fines for violation of data protection laws highly vary. Furthermore, instead of only imposing fines and administrative sanctions, DPAs should be empowered to skim off profits of the data controller that she gained by violation of data protection laws. This amount may be based on estimation.

Moreover, we would advocate to grant the national DPAs an own right of action in front of the courts. The directive requires the independence of the DPAs, but in case of a judicial review of the DPA's sanctions, only a public prosecutor has the right of action in several Member States. This may be problematic, if the public prosecutor lacks data protection expertise. If an own right of action is not possible in all Member States due to national sovereignty in regard to procedural law, the DPAs must at least be granted the right to be heard in front of the court.

2.1.8 Harmonising Processing Notification Procedures

The "whether" and "how" of data processing registration by local data protection authorities is another point that is a major obstacle for service providers. The partially significant diversities in the individual EU member states are perceived as unnecessarily complex and cumbersome. Thus, there is a demand to restrict the requirement of notification on a risk-assessing basis, e.g. to cases of sensitive data concerned. Also, unifying the detailed requirements EU-wide would also lift much of the data controller's administrative burden.²⁷

2.1.9 Empowering Data Subjects and Improving Enforcement

A crucial element of adequate data protection is the empowering of data subjects and the establishment of effective and doable enforcement possibilities. The Article 29 Working Party listed some class action procedures that may facilitate a better application of European data protection principles to data processing activities of any kind. Such procedures may be:

- Improved transparency²⁸
- effective regress mechanisms²⁹
- easily accessible complaints procedures

²⁷ cf. Article 29 Working Party, WP 168 p. 21.

²⁸ See also Privacy International - Response to the European Commission's Communication on the "Comprehensive Approach on Personal Data Protection in the European Union", published January 2011, p.5 f. https://www.privacyinternational.org/sites/privacyinternational.org/files/pi_response.pdf .

²⁹ See the Commission's Communication "A comprehensive approach on personal data protection in the European Union", COM (2010) 609 final, adopted on 04.11.2010, p. 9.

- mandatory privacy breach notification³⁰
- compensation for data loss and privacy breaches, lump sum compensation if damage is not financially measurable³¹

A key element is the introduction of a mandatory data breach notification regulation, whereas it may be desirable to establish not only an obligation of this kind towards the local data protection authorities, but also towards the concerned individuals. However, possible exceptions or case-related restrictions for depending on the potential impact and damage of the breach situation. A less restrict solution for unsubstantial breaches may be thinkable to avoid "notification fatigue" on the side of service customers. Moreover, the establishment of more effective enforcement measures is a very good long-term tool to achieve enhanced data protection compliance of service providers in the first place. Such a measure could also be the introduction of an extended authority for local DPAs/ICOs to be a proxy for individuals in court, for instance in cases of litigation claims. Moreover, the amplified use of fining powers may force service providers to more intensively strive for data protection compliance within their own data processing operations.³² Thus, the restriction on such monetary fining powers, such as in the UK recently³³, significantly hinders the impact of such an enforcement aspect. Desirable may be further clarification on the provisions for damage compensation towards data subjects. The definition of the term "damage" needs further refinement to clarify its scope and to determine how substantial it must be to trigger penalties. Furthermore, the work of the Article 29 Working Party could be made more transparent to increase the general awareness and impact of DPA's actions in the context of specific legal issues.³⁴

2.1.10 Redesign of the Adequacy Process

The verification and acceptance process in respect of a third country's adequate level of protection for the personal data of individuals needs more refinement and clarification. International agreements, such as the existing EU-US Safe Harbor agreement, need evaluation and eventual adaption to the realities of data processing in such an international context. More precise criteria and tighter enforcement actions may provide appropriate instruments to assert the compliance with European data protection rules.

³⁰ This is also supported by the Article 29 Working Party; see WP 184, Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments, adopted on 5 April 2011, p. 9f.

³¹ The possibility to claim immaterial damages required by the Directive 95/46/EC has not been implemented sufficiently by all member states, see Article 29 Working Party, WP 168 p. 17.

³² This approach is increasingly pursued in different European countries, cf. the examples of Spain, Italy and United Kingdom presented by Emily Leach, Data Protection Authorities Crack Down on Breach Offenders, published 09.08.2011 on the website of the International Association of Privacy Professionals, https://www.privacyassociation.org/publications/data_protection_authorities_crack_down_on_breach_offenders.

³³ Cf. the Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998, http://www.ico.gov.uk/~media/documents/library/Corporate/Research_and_reports/guidance_issue_of_monetary_penalties_draft_for_consultation.pdf

³⁴ See the Commission's Communication "A comprehensive approach on personal data protection in the European Union", COM (2010) 609 final, adopted on 04.11.2010, p. 17 f.

Endeavouring towards satisfactory regulations for such international agreements is very much desirable to enable a free flow of data on the international market whilst still maintaining and fostering the protection of individual's fundamental rights. Thus, cooperation with and between international data protection authorities, respectively encouraging and supporting the establishment of such authorities in the first place may also be helpful to achieve this goal.³⁵

2.1.11 Additional Discussion Points

Further potential changes to the European Data Protection Directive being sustainable to enhance and guarantee the realisation of its general principles are discussable. Such changes would be a clarification about ownership of data. This might help to strengthen citizen's rights and advance the enforcement of these. However, another point, the repeatedly raised point of the extension of the scope of the European data protection framework in favour of legal persons must be considered as detrimental to the purpose and basic thoughts of data protection and privacy. These basic principles have emerged from historical development and the experiences of misuse and abuse of personal data against political opponents as well as against social, racial, religious or other vulnerable minorities. Thus, the provisions of the Directive are fundamental grounds tightly bound to the protection of individuals. Only thinkable would be the action of enterprises on behalf of their concerned employees in litigation cases. However, this does not require any change on the current legal framework since this is an aspect that is already sufficiently regulated by the general provisions of legal authorisation and proxy representation in court.

2.1.12 Modification of the EU Standard Contractual Clauses

Beyond the amendments that could be made to the European Data Protection Directive, the EU Standard Contractual Clauses also may be improved by certain alterations and supplementary details. The European Commission established several sets of clauses, focusing on two different constellations of data transfers:

- Transfer of data from controller to another controller (C2C constellation), enshrined in the following two usable versions:
 - Version 2001/497/EC (Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC) and alternatively,
 - Version 2004/915/EC (Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC)
- Transfer of data from controller to a processor (C2P constellation), manifested in
 - Version 2010/87/EU (Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council), repealing its former version of 2002.

³⁵ Article 29 Working Party, WP 168 p. 11.

In our analysis of the EU SCC in D1.2.2 ("Cloud Computing: Legal Analysis"), we already emphasised that within the C2C (controller to controller) constellation, the newer 2004 version is often preferred over the 2001 version due to much more flexibility regarding constantly changing businesses, contracts partners and processing operations. The newer set also introduced a liability scheme depending on causal damage despite the joint liability stipulated in the 2001 set. Though the earlier 2001 version of the clauses provided an indemnity system, it was assessed as very unwieldy and thus the causal, incident-based liability is mostly seen as much more correlating with the realities of day-to-day businesses. In relation to the C2P (controller to processor) constellations, the new 2010 set was much welcomed due to the fact it introduced regulations for sub-processing operations, which were neglected in the older version.

These EU Standard Contractual Clauses however, do not explicitly clarify the means of application regarding the sometimes quite divergent data security requirements of the individual EU member states. Thus, the contract parties may have difficulties to find a solution for such regulations, since these Standard Contractual Clauses may not be altered without them becoming invalid and enforceable. In this context, businesses assessing these clauses for potential use also generally asked for more harmonisation on standards. Manifesting such harmonised standards in this contractual solution is deemed as very desirable to avoid legal and technical uncertainties.

The industry furthermore complained about disproportionate bureaucratic formalities to get the usage of the clauses approved by data protection authorities. In particular for the C2C 2004 set, the approval procedure is not sufficiently harmonised since the DPAs have different views on the requirements of approval. While some DPAs do not even request the official approval of usage by their authority, others demand the information and fulfilment of certain requirements that may differ from country to country (e. g. Germany and the UK). Hence, it is quite difficult and costly for companies to pass through the approval procedure in each EU member country in which the contract shall apply.

Beyond these difficulties of approval, the usability of the EU SCC for multiple layers of parties is limited. In such cases, the clauses are fairly unhandy because each exporting and each importing party has to sign them. This way, a potentially confusing cobweb of contracts is created. When using multilateral contracts, the signing of many parties can still prove very complicated to arrange and manage. Additionally, businesses see a problem with branch offices and company subsidiaries that are not to be considered as separate legal entities since they cannot sign the contract as an independent party.

In the light of these obstacles, there is the question, which incentives could be developed to encourage businesses to use the European Standard Contractual Clauses and still maintain the adequate protection of personal data on the basis of the European data protection framework. Generally, the harmonisation of the European data protection framework, binding for all member states would already mean a significant relief for businesses providing their services within the community area. Nevertheless, not all of the obstacles brought forward by businesses can be removed because further weakening of the protective effects of the European legal framework must be avoided. For instance, the mandatory requirement of each party being obliged to sign the contract is an absolute necessity to warrant legal protection and certainty for the concerned individuals, respectively the service customers. The protection level in respect to the personal data in question must extend over all parties, more precisely, to all controllers, processors and sub-processors involved. This may only be achieved by committing all layers of involved parties to an adequate level of protection contractually.

Requirements of data security and related industry standards may be difficult to regulate in statutory frameworks and thus, it is thinkable that these may be created and implemented industry-led and manifested contractually. However, the development of such standards can

be supported by the enabling of contractual regulation in an annex to the European Standard Contractual Clauses.

2.1.13 Further Development of BCR

Binding Corporate Rules (BCR) are a way for companies to achieve the adequate protection of personal data in cases of in-house (company-group internal) data transfers. Thus, they are of particular interest for company groups that operate multinational and use self-regulating structures to achieve compliance with legal requirements. The EU Data Protection Directive 95/46/EC did not take the use of BCR into account as an explicit way to enable 'such multinational data transfers. They are however, governed by the term other "legitimate grounds" under Article 26 of the Directive 95/46 EC (e.g. SCC or individual contractual solution approved by the concerned DPA).³⁶

As a result of this omission, the approval of BCR demands the approval of all DPAs in the concerned Member States. This administrative burden transfers into a major drawback for corporations to establish BCR. The process of gaining approval of all concerned DPAs with oftentimes different requirements is time consuming and costly. Therefore, it is necessary to streamline and shorten the process to make the implementation of BCR more attractive.

The most obvious approach would be the extension of the "Mutual Recognition" procedure that several national DPAs have established.³⁷ Though WP 74 of the Article 29 Working Party states that the DPAs are authorised to deal with applications in the way it fits best with their national law, several DPAs have agreed to mutually recognise the approval of the lead DPA. This facilitates the application process because the applicant only has one DPA as a discussion partner. To this day, 19 countries take part in this Mutual Recognition. Not all DPAs have sufficient personnel resources to deal with the complex applications. Therefore, the extension of Mutual Recognition might ease the approval procedure for these DPAs. Conversely, the lead DPA should be rewarded with a financial compensation for the additional work. It could be conceivable to raise a fund from all Member States, administered by the Article 29 Working Party to address this need for compensation.

A problem in streamlining the Mutual Recognition procedure is that in some Member States the national law does not allow unilateral declarations as a binding self-commitment. Until now the applicant had to find an additional solution to the BCR which is enforceable in these states. This gap in the approval procedure may be closed by implementing the concept of BCR in the European legal framework.

The reason for the reluctance of multinational corporations to apply for BCR extends beyond only the administrative complexity. The BCR oftentimes do not fit their needs. The current shape of BCR does not reflect two major issues:

- 1) Corporations criticise that BCR cannot be used for data transfer to companies outside the corporate group ("onward transfers"). A possible solution for this gap could be the introduction of "Binding Business Venture Rules" that cover also onward data transfer to permanent affiliates outside of the main corporation.

³⁶ Article 29 Working Party, WP 74, Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3rd June 2003, p. 9.

³⁷ Please refer to D1.2.2 for details on the procedure.

- 2) The Condition sine qua non for such an extension of the nature of BCR is the internal and external enforceability³⁸ in regard to these affiliates. They must be bound by the "Binding Business Venture Rules" the same way the main corporation is bound by BCR now. Under these conditions this concept may also apply to a larger network of companies.

2.2 Conclusion and Outlook to Supplementary Means

The European Standard Contractual Clauses and Binding Corporate Rules are helpful instruments to enable a free flow of data especially in transborder processing contexts. Nevertheless, they are significantly in need of an adequate adaption to current technological developments that often entail a multitude of involved parties and rapidly changing conditions regarding contract partners and processing operations. However, an advancement of these tools must come along with a similarly effective accommodation of the European Data Protection Directive 95/46/EC. This is an absolute necessity to encounter shortcomings that are rolled out through the eminent changes of the modern world, entailing the expanding usage of IT services throughout all social strata and classes of society. The growing relevance of Web 2.0 and the provision of every conceivable means to access IT services, e.g. via cloud computing, challenges the traditional approach of protection of personal data. Thus, the core objectives of European data protection principles demand considerable changes especially concerning uncertainties of role allocation (Data controller/processor determination), jurisdiction and enforcement aspects. Foremost, these changes will have to be tackled on the level of these legal adoptions we have introduced in this document. Nonetheless, supplementary means on the technological level may support these adaptations and further enhance the protection of personal data in the European Union. The deployment of classical as well as new technical possibilities, such as homomorphic encryption, or principles of multi-cloud architectures may provide good opportunities to warrant such an enhancement as built-in-solutions right from the start.

³⁸ Please refer to TClouds Deliverable D1.2.2. for further information.

Chapter 3

Outlook on Future Development

3.1 Proposed Data Protection Regulation

The upcoming shift in European data protection from a Directive to a directly binding Regulation will have significant impact on the harmonisation of data protection in the EU. All member states will need to adhere to the same rules.

The draft³⁹ already addresses some of the aforementioned gaps of the Directive, such as harmonisation of procedures and establishing Privacy by Design and Privacy by Default.

Commissioner Kroes stated that the Regulation was meant to enable lawful cloud computing in the EU.⁴⁰ In the current version of the draft this is doubtful. The Regulation would surely unify the market within Europe but is capable to open protection gaps on the applicability and international transfer. The regulation shall be applicable whenever a service provider offers its services to an EU customer. This seems to be especially privacy friendly and first sight but it most probably would be not enforceable.

"Uncertainty will persist as to whether particular non-European cloud providers and cloud users are regulated in the EU and, if so, which law(s) will apply to them. This may discourage the development of EU data centres and the use of EU cloud services generally"⁴¹ stated Christopher Millard, leader of the Cloud Legal Project at Queen Mary, University of London.

Though criticised as unnecessary administrative burden, the mandatory Privacy Impact Assessment (PIA) could prove to be beneficial for the cloud business. As of today risk assessments need to be considered best practice before providing or using a cloud service. An assessment with a focus on privacy risks instead of only economical or security risks could lead to innovations and competitive advantage regarding security measures of a CSP.

³⁹ Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 (final), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf January 25th 2012

⁴⁰ Neelie Kroes - Setting up the European Cloud Partnership, http://europa.eu/rapid/press-release_SPEECH-12-38_en.htm?locale=en World Economic Forum Davos, Switzerland, 26th January

⁴¹ Christopher Millard, leader of the Cloud Legal Project at Queen Mary, University of London, <http://www.qmul.ac.uk/media/news/items/hss/63123.html>

3.2 European Cloud Computing Strategy

Outlined in a speech by commissioner Kroes in January in Davos⁴², the European Commission finally published its long awaited Cloud Strategy on September 27th 2012.⁴³

The strategy intends to boost the cloud business and cloud usage in the EU since the EC expects massive economic growth from utilising cloud infrastructures and services.

As of today, European customers have been hesitantly in using cloud services. Accordingly, the global market is dominated by US-based CSPs. The EC therefore makes a political commitment to facilitate cloud computing and aims at “enabling and facilitating faster adoption of cloud computing throughout all sectors of the economy which can cut ICT costs, and when combined with new digital business practices, can boost productivity, growth and jobs”.⁴⁴

Scope of the Strategy document is to set out “the most important and urgent additional actions”.⁴⁵ For this purpose the EC identifies three key areas to take actions in:⁴⁶

1. Harmonisation of the European market

The EC considers the different national implementations of European Directives into national law and the uncertainties to be a significant hindrance for establishing trustworthy cloud services.

2. Evaluation of standards

The “jungle of standards” has created confusion. The existing standards have to be evaluated and reviewed.

3. Problems with contracts

Concerns about contractual matters such as portability, liability, change control and compensation need to be solved in order for users to take confidence in fair contracts.

The EC states to have taken considerable steps with regard to unifying the EU market, as many of the necessary harmonisation steps were already part of the Single Market Pillar of the Digital Agenda for Europe and the Single Market Act.⁴⁷

The actions taken include the proposal of a uniform legal Regulation for **data protection** (see above). “Given that data protection concerns were identified as one of the most serious

⁴² Neelie Kroes - Setting up the European Cloud Partnership, http://europa.eu/rapid/press-release_SPEECH-12-38_en.htm?locale=en World Economic Forum Davos, Switzerland, 26th January 2012

⁴³ Website for the European Cloud Computing Strategy http://ec.europa.eu/information_society/activities/cloudcomputing/cloud_strategy/index_en.htm

⁴⁴ European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 2.

⁴⁵ European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 2.

⁴⁶ Interestingly, these three key areas mirror the structure and composition of this document D1.2.3 Solutions and Enablers.

⁴⁷ European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 6.

barriers to cloud computing take-up, it is all the more important that Council and Parliament work swiftly towards the adoption of the proposed regulation as soon as possible in 2013.”⁴⁸

A second objective is to “simplify **copyright clearance, management and cross-border licensing**”.⁴⁹ In this sector the EC proposed a Directive on Orphan Works COM(2011) 289; a Directive on Collective Rights Management COM(2012) 372, and to review of the Directive on Re-Use of Public Sector Information, COM(2011) 877. Furthermore, an ongoing multi-stakeholder mediation process is taking place facing the licensing issue in trans-border cloud services.⁵⁰

Additionally, the EC announced to address general cyber security challenges in its “Strategy for Cyber Security” in the coming months, indicating inter alia to “appropriate technical and organisational measures that should be taken to manage **security risks**”.⁵¹

Apart from unifying the single market the EC sees the need for “a chain of confidence-building steps to create trust in cloud solutions”.⁵² To make progress on this the EC launches three cloud-specific key actions:

1. Key Action 1: Cutting through the jungle of standards⁵³

- Promote trusted and reliable cloud offerings by tasking the European Telecommunications Standards Institute (ETSI) to coordinate with stakeholders to identify by 2013 a detailed map of the necessary standards (inter alia for security, interoperability, data portability and reversibility).
- Enhance trust in cloud computing services by recognising at EU-level technical specifications in the field of information and communication technologies for the protection of personal information in accordance with the new Regulation on European Standardisation.
- Work with the support of ENISA and other relevant bodies to assist the development of EU-wide voluntary certification schemes in the area of cloud computing (including as regards data protection) and establish a list of such schemes by 2014.
- Address the environmental challenges of increased cloud use by agreeing, with industry, harmonised metrics for the energy consumption, water consumption and carbon emissions of cloud services by 2014

⁴⁸ European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 8.

⁴⁹ European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 8.

⁵⁰ European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 7.

⁵¹ European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 8.

⁵² European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 9.

⁵³ European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 10,11.

2. Key Action 2: Safe and fair contract terms and conditions⁵⁴

- Develop with the involvement of stakeholders model terms for cloud computing service level agreements for contracts between cloud providers and professional cloud users, taking into account the developing EU acquis (sic) in this field by 2013
- Propose to consumers and SMEs model contract terms and conditions by 2013, standardizing key contract terms and conditions⁵⁵, providing best practice contract terms for cloud services on aspects related with the supply of "digital content"
- Reviewing standard contractual clauses applicable to transfer of personal data to third countries and adapting them, as needed, to cloud services; and by calling upon national data protection authorities to approve Binding Corporate Rules for cloud providers
- Agree with industry on a code of conduct for cloud computing providers to support a uniform application of data protection rules⁵⁶

3. Key Action 3: Establishing a European Cloud Partnership (ECP) to drive innovation and growth from the public sector⁵⁷

- Establish an umbrella for national cloud initiatives at Member State level, such as G-Cloud in the UK, Trusted Cloud in Germany and Andromede in France to:
- identify public sector cloud requirements; develop specifications for IT procurement and procure reference implementations to demonstrate conformance and performance
- Advance towards joint procurement of cloud computing services by public bodies based on the emerging common user requirements.

The EC has presented a very ambitious strategy for the next two years. Surprisingly, licensing as well as sales issues were addressed with the same regard as data protection and security issues. The intent to establish model contract clauses and certification schemes seems auspicious from a privacy advocate's point of view, although it immediately has been severely criticized by US stakeholders as the "Rise of E-Fortress Europe"⁵⁸.

However, worthy of criticism is the lack of engagement of the Art. 29 Working Party. It is worrisome when the EC writes that code of conduct for CSP to support a uniform application of data protection rules may be submitted to the Article 29 Working Party for endorsement afterwards. Involving the Art.29 Working Party already in drafting process with the industry would ensure that the data subject's and consumer's rights are considered.

⁵⁴ European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 11-13.

⁵⁵ fFr those cloud-related issues that lie beyond the Common European Sales Law the EC will set up an expert group.

⁵⁶ These may be submitted to the Article 29 Working Party for endorsement in order to ensure legal certainty and coherence between the code of conduct and EU law.

⁵⁷ European Commission - Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf page 13, 14.

⁵⁸ Richard Adhikari, EU Cloud Strategy Ruffles US Industry Group's Feathers, E-Commerce Times, September 27th 2012, <http://www.ecommercetimes.com/story/76264.html>

Chapter 4

Contractual Enablers

As stated in the Article 29 Working Party Opinion 1/201012 on the concepts of controller and processor, “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”.⁵⁹ If the customer cannot negotiate an individual contract with a CSP, he has to carefully choose a CSP providing SLA that allows for compliance with the customer’s legal requirements. The customer has to prove the due diligence; otherwise he could be liable for faulty selection of his processor (*culpa in eligendo*). Therefore the following contractual topics apply for the negotiation of an individual contract as well as the selection of a CSP with suitable SLA.

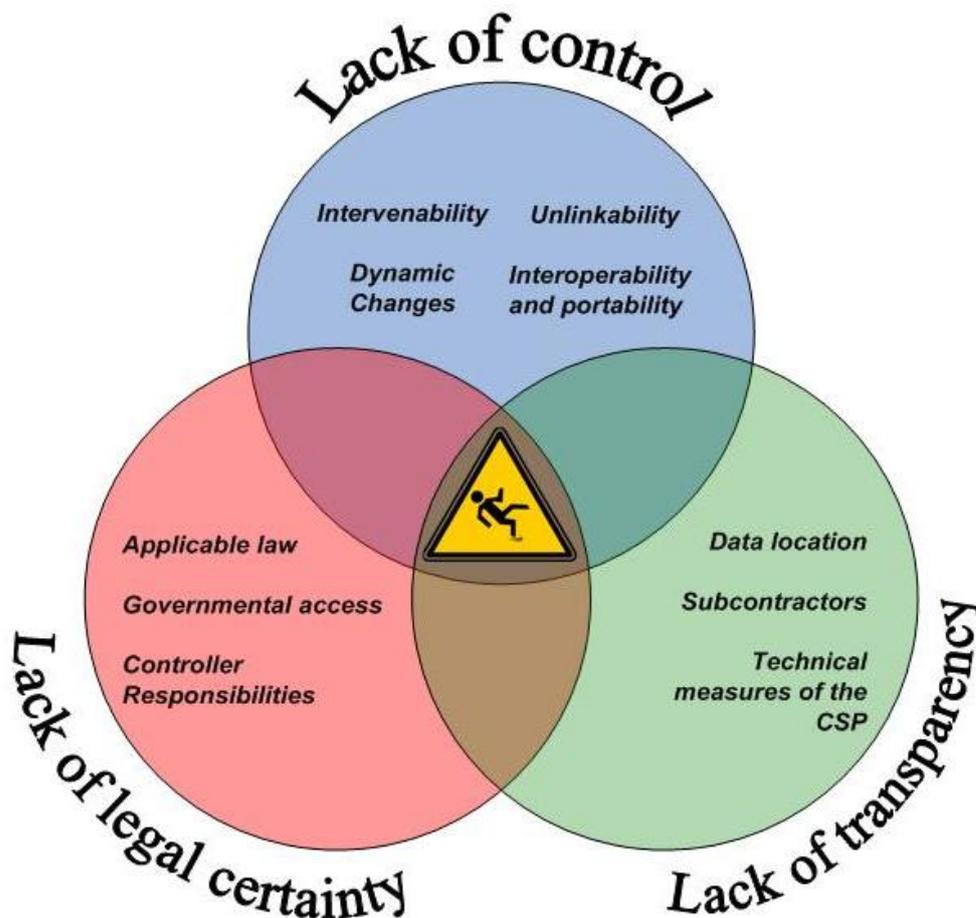


Figure 2 Cloud computing specific risks

⁵⁹ Opinion 1/2010 on the concepts of "controller" and "processor" - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

4.1 Individual Contracts and SLA

Before deciding on which cloud service to use, be it public or private, IaaS, PaaS, or SaaS, the customer needs to conduct a risk assessment. This risk assessment is not only best practice but will become legally mandatory in form of a Privacy Risk Assessment in the proposed European Data Protection Regulation. A proper risk assessment before “going cloud” means to identify one's internal processes and the relevant information involved in these processes, a risk and threat analysis, as well as identifying legal compliance requirements that have to be met and the necessary safeguards to be installed. The outcome of such a risk assessment may be that not all of an enterprise's processes are suitable for a public cloud or not yet cloud-ready. A risk assessment additionally helps to evaluate security means provided by the CSP and identify own responsibilities with regard to the cloud service.

The TClouds project will provide a comprehensive Privacy Impact Assessment in 2013 in the document D1.2.4.

Table 1: Legal Responsibilities

Legal Responsibilities	Customer	CSP	Subcontractor of the CSP
Legal role	data controller	data processor	sub-processor
Legal foundation for the processing of PII			
Absence of legal limitations for IT outsourcing⁶⁰			
Selection of CSP			
Selection of subcontractors		 ⁶¹	
Comprehensive formal contract for cloud services		 ⁶²	
Technical and organizational security measures		 ⁶³	 ⁶⁴

⁶⁰ National legislation may pose restriction on the option to outsource data processing due to professional secrecy, highly sensitive data or governmental secrecy obligations.

⁶¹ This depends on whether the CSP is subject to EU law.

⁶² The CSP might not have legal responsibility to establish a comprehensive contract with his subcontractors but he should be contractually obliged by the customer to relay its own duties to the subcontractors.

⁶³ This depends on whether the CSP is subject to EU law. If yes, the CSP faces requirements on processors, Art. 17(1) Data Protection Directive 95/46/EC.

Legal Responsibilities	Customer	CSP	Subcontractor of the CSP
Control of CSP			
Control of subcontractors			
Data subject's rights			
Lawfulness of data transfer to outside of the EEA		 ⁶⁵	 ⁶⁶
Liability for data breaches			
Law enforcement access			

Legend:  yes;  no;  probably, but could not be verified

4.1.1 Scope of the Contract

Independent from the service layer, a cloud service contract has to specify the subject matter of the contract. What exactly does the customer pay for and which resources and services does the CSP provide. Furthermore the contract has to include all mutual obligations. Additional essentialia negotii are the fee and the duration for the service duration.

4.1.2 Data Protection and Data Security Topics

4.1.2.1 Involved Data and Purpose Specification

According to Article 17 (3) of the Data Protection Directive 95/46/EC, the customer is obliged to sign a contract or legal act binding the processor. In web-accessed cloud businesses this means that the customer needs to establish a formal contract with the CSP that is well documented.

The baseline principle of European Data Protection laws is the purpose specification and limitation.⁶⁷ This principle demands that personal data must only be collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with

⁶⁴ This depends on whether the CSP is subject to EU law. If yes, the CSP faces requirements on processors, Art. 17(1) Data Protection Directive 95/46/EC.

⁶⁵ If he is based within the EEA and uses a subcontractor from outside of the EEA.

⁶⁶ If he is based within the EEA and uses a subcontractor from outside of the EEA.

⁶⁷ Article 6(b) of the Data Protection Directive 95/46/EC.

those purposes.⁶⁸ Therefore, the first stage to achieve data protection compliance with this contract is to determine the type of data which is to be transferred to the cloud and lay down the purpose of the processing of personal data from the data subject.

4.1.2.2 Location of Facilities

The first and main connecting factor for the applicability of the EU Data Protection Directive 95/46/EC regarding CSPs is the establishment of facilities within the EEA. The highly virtualized, dynamic and oftentimes borderless nature of cloud computing contradicts this more static jurisdictional approach. This leads to several issues that need to be contractually addressed.

A globally operating CSP may, and probably will, establish data centres in different countries, maybe even on different continents. This leads to a different applicable national law, jurisdiction and competent government authorities for every data centre. Without adequate transparency on the location of these data centres the customer is unable to conduct a risk assessment. He does not have a chance to make a choice to ban some data centres contractually. If the customer cannot evaluate to local laws he cannot be sure whether his data is not transferred to a third party state which does not provide an adequate level of data protection. It is therefore necessary that the CSP gives transparent information about where his data centres are located at least at country granularity.

An accompanying issue which is often neglected in this context is the administration of the CSP. The administration personnel accessing the cloud resources is data transfer itself. If an administrator operating from India accesses cloud resources in France, this is considered a data transfer to a third party state. A customer with special geographical requirements therefore needs to contractually ensure that the competent personnel is located in the same area.

4.1.2.3 Transborder Transfer of Data

Transborder data transfer to outside of the EEA or other states with adequate level of protection needs a specific contractual basis⁶⁹ (e.g. Standard Contractual Clauses, Binding Corporate Rules). The customer has to evaluate or negotiate what this contractual basis is and if additional contractual measures are necessary.

4.1.2.4 Confidentiality of the CSP

As data processor, a CSP must ensure confidentiality. The general confidentiality requirement for all processing activities is based on Article 16 of the Data Protection Directive 95/46 EC: *“Any persons acting under the authority of the controller or of the processor, including the processors themselves, who have access to personal data, must not process them except on instructions from the controller, unless he is required to do so by law.”*⁷⁰

If the CSP is based outside the EEA, the customer may want to ensure this confidentiality by contractual means.⁷¹ Such a contractual clause is considered best practice even if the CSP is

⁶⁸ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 11

⁶⁹ Please refer to D1.2.2 for further information.

⁷⁰ Art. 16 “Confidentiality of processing” of Directive 95/46/EC.

⁷¹ Supporting a contractual clause on confidentiality: CNIL - Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing, http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

an EU-based company not only for reasons of data protection but to protect his business secrets.

Exemplary clause:

The processor (CSP) shall not disclose directly or indirectly any information regarding without limitation the customer's business, processes, documents, personal and other data or any communication between the parties.

This clause can be extended by exemption clauses for confidentiality breaches required by law, e.g. governmental access (see below).

As a processor, the CSP also must not be able to access data at will. He should solely act on behalf of the customer. This contradicts common cloud practices as decency checks or profiling for marketing reasons are commonplace.

4.1.2.5 Notification of Governmental Access

Related to the issue of confidentiality is the widely discussed concern about governmental access to data processed or stored in the cloud. Especially in cross-border operating clouds this is a valid concern of potential customers. If the CSP has established data centres in several foreign countries then several national laws and jurisdictions are applicable. The conditions for law enforcement agencies getting access may vary greatly. Even within the EU the competent authorities and their prerequisites are considerably different.⁷²

Unless it is otherwise prohibited, the CSP should have the obligation to inform his customer about governmental or court access requests and whether they were granted.

4.1.2.6 Subcontractors

Cloud Computing business models oftentimes involve a number of subcontracting (cloud) service providers. On behalf of the first processor, these subcontractors become subprocessors if they gain access to customer's data. *"All the relevant obligations must therefore apply also to the sub-processors through contracts between the cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider."*⁷³ The customer may want to include a clause that obliges the CSP to relay his own contractual and legal obligations regarding the customer's data to his subcontractors.

It is subject to an ongoing discussion if and to what degree the CSP needs to provide transparency about his subcontractors. Without doubt, outsourcing is part of the entrepreneurial freedom of the CSP. But a growing chain of subprocessors and subsubprocessors may hinder governance and effective control for the customer.

The Article 29 Working Party demands full transparency and additionally the consent of cloud customer for all subprocessors: *"the processor can subcontract its activities only on the basis of the consent of the controller, which may be generally given at the beginning of the service with a clear duty for the processor to inform the controller of any intended changes concerning the addition or replacement of subcontractors with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned."*⁷⁴

⁷² The TClouds project shall work on a comparative analysis of these differences in D1.2.4 "Privacy Impact Assessment" in 2013.

⁷³ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 9.

⁷⁴ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 10.

A chain of subprocessors also raises subsequent questions of liability. The customer needs to determine who shall be liable in case of a breach occurring at the subprocessor. If the situation is unclear the customer has to take the necessary precautions by negotiating a contractual liability of either the CSP directly or of the subcontractor via a transfer of the liability based on the contract between the CSP and the subcontractor.

4.1.2.7 Control and Intervenability

Since the customer is legally responsible for granting and enforcing the data subject's rights, it is important that the customer contractually ensures that he is able to give instructions to the CSP. This control functionality does not necessarily need to have high impact on the CSP's architecture. More important is that the control to e.g. grant or revoke access profiles and order the start and stop of processing remains with the customer. The data subject's rights include access to the data and the option to correct or delete incorrect data. The CSP should assist and support the customer in complying with these data subject's rights. According to the Article 29 Working Party the extent and modality of this assistance should be clarified within a contract.⁷⁵

4.1.2.8 Change Notification

Changes in the cloud or service architecture can have a major impact on the customer. Therefore, it is necessary to contractually impose a notification obligation on the CSP. Important is that the necessary notification of relevant changes is upfront by a certain amount of time (change notice time). What *relevant changes* are depends on the specific case but may include changes affecting the certification status of the CSP or the customer, the applicable jurisdiction, data centre location, the company ownership of the CSP, or major system changes such as the implementation of additional functions.

4.1.2.9 Breach Notification

The contract should include a notification obligation with regard to a breach of the customer's data. The contract should also specify the maximum time frame and the communication channel for such a notification.

4.1.2.10 Deletion

In virtualized environments the customer faces special problems regarding the retrieval or deletion of data. "*Secure erasure of personal data requires that either the storage media to be destroyed or demagnetised or the stored personal data is deleted effectively through overwriting.*"⁷⁶ This does not apply to all stages of cloud usage. Oftentimes the data will not be persistently stored because of the virtualisation.

The contract needs to ensure that the data is erased securely at the instruction of the customer or when the service is concluded.⁷⁷ This requirement applies to all storage media: regular VMs, back-ups, redundant copies for availability, previous versions, temporary files and even file fragments.⁷⁸

⁷⁵ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 9.

⁷⁶ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 12.

⁷⁷ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 13.

⁷⁸ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 13.

For some issues touched here, the legal community has not found satisfactory answers yet.

Regarding deletion of back-up and log data one has to weigh the data subject's interest against the integrity requirements. The Article 29 Working party mandates the secure deletion in back-ups and logs in every case, strictly applying the Data Protection Directive that demands "erasure"⁷⁹ The UK Information Commissioner's Office (ICO) takes a different view, arguing that it is not always possible to securely delete data.⁸⁰ The ICO considers suggests that putting data "beyond use" may be sufficient and that the ICO will not take any enforcement actions against organisations that retain such data as long as specific safeguards are in place.⁸¹

- The data controller is not able, or will not attempt, to use the personal data in any way that affects the data subject
- The data controller does not give any other organisation access to the personal data
- The personal data is protected by appropriate technical and organisational security means
- The data controller commits to permanent deletion of the information if, or when, this becomes possible.

The authors of this deliverable prefer a case by case evaluation, clearly demanding the cloud customer to take comprehensive contractual and technical precautions to as far as technically possible completely delete personal data even from back-ups. This requires the customer to have an effective information management and the CSP to offer information about automatically created back-ups and copies.

A second issue is the lawful erasure of encrypted data. There is a disagreement whether it can be considered sufficient to merely destroy the key and not touch the data itself. The authors of this document tend to disagree. Since encrypted data is not rendered anonymous, the legal requirements for personal data still apply. We will focus on this question in D1.2.4 "Privacy Impact Assessment" in 2013.

The customer should make sure that the contract addresses deletion of data and gives a clear provision for the CSP as well as possible subcontractors.

It is the customer's own responsibility to block access to data which is no longer needed for the predefined purpose but has to be stored due to retention requirements.

4.1.2.11 Decency Checks

Some SLAs include a notification that the CSP carries out decency checks or other automated scanning of uploaded data to identify data that is not in accordance with the CSP's policy. This could refer to copyright infringement as well as content considered immoral such as nudity pictures.

These scans of data, which are not publicly available but confidential, contradict data protection requirements. Since a notice and takedown approach is not feasible in these

⁷⁹ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 13.

⁸⁰ ICO – Deleting Personal Data, http://www.ico.gov.uk/for_organisations/guidance_index/~/_media/documents/library/Data_Protection/Practical_application/deleting_personal_data.ashx

⁸¹ ICO – Deleting Personal Data, http://www.ico.gov.uk/for_organisations/guidance_index/~/_media/documents/library/Data_Protection/Practical_application/deleting_personal_data.ashx

cases this has to be considered anticipatory obedience of the CSP. Indisputably, the CSP has every right to establish own policies and enforce them, but he needs to give potential customers transparent information on this matter since it is irreconcilable with confidentiality obligations.

4.1.3 Technical Security Measures

According to Art. 17 (1) of the Data Protection Directive 95/46/EC, the CSP as a data processor has to provide adequate technical and organisational security measures. Since both parties face legal requirements it is important to specify a baseline of security measures in a contract. This baseline depends on the identified risks regarding the sort of data and the specific processing operations. The Article 29 Working Party even requires that concrete technical and organizational measures are specified within the contract.

4.1.3.1 Isolation

The very key aspect of cloud computing is the shared use of a pool of resources using virtualisation. Due to this sharing, isolation is an essential precondition for multi-tenancy. But the grade to which isolation is implemented and safeguarded may differ.

The isolation requirements also depend on the sensitivity of the data and processes and legal requirements for the customer. This can lead to a complete isolation on hardware level.

As one example, the Amazon GovCloud⁸² implements severe restrictions in terms of separation, e.g. being a completely separate cloud dedicated to the U.S. government, and being used to implement government services only. Furthermore, all individuals working at the GovCloud data centres are required to be American citizens, and are required to agree not to disclose any information regarding the GovCloud to non-American citizens.

Since isolation is solely in the domain of the CSP, it is recommended that the contract specifies what the CSP does to safeguard multi-tenancy (management of shared resources and hypervisor). Since this may infringe business secrets of the CSP a baseline should be sufficient.

Isolation also touches on proper access and rights management. The roles within the CSP and the customer should be regularly revisited and no roles should have excessive access privileges (e.g. administrators).

4.1.3.2 Monitoring

The customer most probably has legal monitoring requirements for compliance. Therefore, the contract should include the customer's rights to monitor the cloud service and specifications to what extent and in which way the customer has to cooperate or provide monitoring tools.

The customer has the responsibility to choose his monitoring tools with consideration of the CSP since, e.g. load tolerance and elasticity monitoring, may diminish the cloud's performance or affect other customers.

4.1.3.3 Logging

For Logging similar considerations as for monitoring apply. Depending on the service layer the customer may install logs himself. If this is not possible, the customer has to negotiate

⁸² Amazon GovCloud <http://aws.amazon.com/govcloud-us/>

what logs the CSP will provide. It has to be contractually specified what will be logged and who will have access to the logs (e.g. the customer might only get derived logs).

4.1.3.4 Encryption

When using a public cloud encrypting the data contributes significantly to enhance confidentiality and isolation. Encryption is to be considered best practice for all data stored in the cloud. Some goes for data in transfer either in or from the cloud and all communications; these should be encrypted and happen via a secure communication channel.⁸³

For encryption the customer needs to take into account three issues:

4. The key management. As the benefits of confidentiality ultimately depend on the techniques of encryption as well as on secure key management. Best practice is not to rely on the encryption service provided by the CSP, but to use customer side encryption methods to have control over confidentiality (even in cases of access request of governmental authorities) and key management.
5. Processing. Although there is promising research⁸⁴ it is not yet feasible to process encrypted data. Therefore, even with proper key management (as the TClouds research on Cryptography as a Service (CaaS) the data needs to be decrypted in the RAM. This leads to the theoretic possibility of attacks.
6. Deletion. Encrypted data is legally not considered anonymized data.⁸⁵ Therefore, for encrypted personal data legal data protection requirements still apply. Strictly interpreting the law even encrypted data needs to be securely deleted. The common practice just to destroy the key and leave the encrypted data as it is would be insufficient. Solving this issue requires further interdisciplinary discussion.

To counter some of these issues the customer should include contractual clauses imposing confidentiality obligations on employees of the CSP and his subcontractors. If the CSP offers an own encryption service the contract should include specifications for secure key management.

4.1.3.5 Availability

The contract needs to specify the uptime guarantees. What is the maximum downtime, it is calculated weekly, monthly or annual? It is also important to specify what is considered as downtime: slow response time, network failure, outage of one or more data centres or availability zones. Additionally it is important to define the point in time from when the outage time is calculated.

Furthermore, the customer should make sure that the availability guarantees apply to all services, including logs and back-ups. He should demand transparency on the high-level character of the technical measures to safeguard availability as redundant storage, back-ups, network elasticity, deduplication, since these may effect the customer's risk assessment.

⁸³ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 15.

⁸⁴ Please refer to chapter 5.2.3.4 for considerations on homomorphic encryption.

⁸⁵ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 15.

4.1.4 General Contractual Topics

4.1.4.1 Disaster Recovery and back-ups

The contract should include mechanisms for disaster recovery. Who is responsible for regularly creating back-ups? Who is responsible for retrieving back-ups, if data is lost for some reason?

4.1.4.2 Business Continuity

The contract should include mechanisms and responsibilities for the case of business failure of the CSP and the customer. E.g. in case of insolvency of the CSP, how long is the customer still able to retrieve his data?

4.1.4.3 Cancellation

The contract should include specifications on how the contract can be cancelled and the service can be terminated by the customer. Additionally, the contract should specify under which circumstances the contract may be terminated by the CSP (e.g. non-payment or breach of obligations) and what will happen to the customer's data in this case.

4.1.4.4 Portability / Vendor lock-in

If the customer decides to leave one CSP to migrate to another he will probably face difficulties due to the lack of widely accepted standard and APIs. The so called vendor lock-in can be contractually mitigated by including restricts the customer in his options to leave a commitment of the CSP CSP and migrate his data to provide standard data formats another provider with more suitable conditions.

The cloud client should check whether and service interfaces facilitating interoperability and how the provider guarantees the portability.⁸⁶ of data and services prior to ordering a cloud service. Additionally, the implementation of standardised or open data formats may be stipulated by contractual clauses.

4.1.4.5 Contractual Penalties

The customer has to identify key aspects in the SLA and check if and under which circumstances there are contractual penalties. Regarding the unbalanced power between an SME customer and a global CSP, penalties are the most effective means to ensure that the CSP meets the SLA obligations.

4.1.4.6 Liability

Most SLAs restrict the liability of the service provider for business losses caused by cloud failure. Common is the limitation to a lump sum per customer (e.g. the fee for 12 months of cloud usage). It is recommended to negotiate a higher sum if the outsourced data and processes are business critical.

4.1.4.7 Place of Jurisdiction

For cross-border operating clouds it reflects the interests of both sides to have an agreement on the place of jurisdiction. Otherwise both face the risks to get sued in any country where the cloud uses facilities.

⁸⁶ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 16.

4.1.4.8 Forensics Cooperation

If litigation and other reasons for necessary access to forensic logs and tools have been identified as reasonable risks, it makes sense to negotiate with the CSP a commitment for cooperation in case the customer has a valid need of forensic data.

4.1.4.9 Intellectual Property

In the case a customer uses an IaaS or PaaS cloud to develop own applications, he needs to check the SLA or contract if the CSP gains any rights regarding the intellectual property on the developed applications.

4.1.4.10 Licensing

Clouds often operate globally, and even if they are regional clouds, they can be accessed from everywhere by the customer. This can raise issues regarding the licensing of used software. The license must not be regionally restricted. Depending on the service layer (IaaS or SaaS) both parties can be affected by this issue. The contract could include a disclaiming of liability for the party that has no influence on the used software and its licenses, respectively.

4.2 Processor BCR

On June 6, 2012, the Article 29 Working Party adopted its long awaited Working Document on elements and principles for Processor Binding Corporate Rules (PBCR, also referred to as “Binding Safe Processor Rules”).⁸⁷

Same as the common BCR Processor BCR are a code of conduct, which is to be implemented internally by a large internationally operating enterprise. They are intended to provide an adequate level of data protection within a company allowing data transfer to outside of the EEA without further contracts or authentication. The longer established BCR⁸⁸ applied to data controllers not enabling globally operating data processors such as CSPs to profit.

Processor BCR could prove to be a vital cloud enabler since they address one of the most crucial issues from a European point of view: the global data flow of borderless clouds. It allows big multinational CSPs to apply to EU customers without reserving only EU facilities for these customers. The implementation of BCR within a globally operating commodity cloud service provider could give this CSP a significant competitive advantage regarding European customers. Using a CSP with authorised PBCR in place is as legally compliant as to using a solely EU cloud without additional contracts allowing the data transfer.

The Working Document sets up a table with requirements and principles for PBCR. Parallel to BCR for controllers the requirements include:

- How to ensure the binding nature of the Processor BCR internally and externally
- The effectiveness based on audits, oversight and training programmes
- Duties for cooperation with the controller and the competent DPAs

⁸⁷ Article 29 Working Party, WP 195, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

⁸⁸ Please refer to Chapter 2.1.13 “Further Development of BCR” of this document.

- A specification of the data processing and the material and geographic scope of the BCR
- An effective management of changes and updating of the BCR
- General data protection safeguards

Since PBCR must be accepted by all competent DPAs, the Article 29 Working Party is working towards a cooperation procedure between the DPAs, similar to that for Controller BCR. It is also drafting an application form.

In the following we will highlight some requirements highly affecting CSPs that want to establish PBCR.

4.2.1 Public Availability

Contractually seen, BCR would be part of the contract between the customer and the CSP implementing the BCR. A CSP is required to reference the BCR in his Service Level Agreements and publish them e.g. on his website.⁸⁹ Therefore, some provisions of the BCR may unfold binding character for the customer as well, depending on how they're phrased.

4.2.2 Liability

A key provision in the PBCR is the processor's (including CSPs) acceptance of a liability for paying compensation for any damages resulting from the breach of BCR.⁹⁰ Liable will be the main EU based member of the processor's corporate group. This member would assume liability for any breach committed by another member of the group or a subprocessor. The liable member therefore has to prove that it has sufficient assets when applying for acceptance of its BCR. In case that the corporation does not have an EU-based member, the corporations headquarter must assume liability.

Additionally, the processor has to grant third-party beneficiary rights to data subjects in the event the data controller factually disappears, ceases to exist in law or becomes insolvent, including judicial remedies and compensation for any breach of the data subject's rights by the processor.⁹¹

4.2.3 Commitment to cooperation

BCR require the processor to commit to cooperation with the controller and European DPAs.⁹² This includes accepting audits by the competent DPA and reasonably assisting the

⁸⁹ Article 29 Working Party, WP 195, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf page 4.

⁹⁰ Article 29 Working Party, WP 195, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf page 4.

⁹¹ Article 29 Working Party, WP 195, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf page 3.

⁹² Article 29 Working Party, WP 195, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf page 7.

controller in complying with data protection laws, including handling complaints and requests of the data subject and responses to DPA inquiries.

For a CSP with multiple customers in the EU this would mean to cooperate with several DPAs. It is therefore absolutely necessary to unify the European data protection framework and standardize the audit procedure.

4.2.4 Transparency on subcontractors

Outsourcing of data processing to subcontractors that are not part of the PBCR is limited. The cloud customer must give his prior consent to this onward transfer to external subcontractors. This can happen via a general consent to subcontracting given when the SLA is agreed upon. In this case the customer still needs to be informed about all subcontractors and all intended replacements or additions of sub processors. For any intended change the customer would have the chance to object or terminate the contract prior to the onward transfer of data.⁹³ The involvement of subcontractors must only happen on basis of a written agreement between the CSP and the subcontractor that the level of protection mirrors the PBCR and SLAs of the CSP.⁹⁴

This requirement could prove to be a major drawback in the highly dynamic cloud market. The PBCR are clearly tailored to processors with small fluctuation among its subcontractors.

⁹³ Article 29 Working Party, WP 195, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf page 10.

⁹⁴ Article 29 Working Party, WP 195, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf page 10.

Chapter 5

Technical Solutions an Enablers

We evaluate four international standards of good and best practices or certification frameworks for cloud computing.

Table 2: Overview of evaluated standards and guidelines

Overview	CSP Baseline Protection	Procure Secure	CSA STAR	EuroCloud Star Audit
Issuer	BSI	ENISA	CSA	EuroCloud
Character	Guidelines	Guidelines	Self-Certification	Certification
Target Audience	CSP	Customer	CSP	CSP
Service Level	All	All	All	SaaS
Number of Questions	85	208	197	ca. 200
Questions Publicly Available				
Public Registry of Answers Available				
Intended Type of Answers	<i>considered or not considered</i>	free text	<i>yes or no</i>	unknown
Answers Formally Verifiable				

Legend:  yes;  no;  probably, but could not be verified;  could not be determined

Probably, all frameworks address a baseline of security requirements. (For the EuroCloud SaaS Star Audit these assumptions were not verifiable.) Apart from this baseline, they all have a different focus and target audience. A detailed and comprehensive framework that addresses all identified key issues is not yet established. The issue of licensing in cloud environments that has been identified in the EC Cloud Strategy is neglected by all frameworks.

Table 3: Overview of addressed key issues

Key Issues Addressed	CSP Baseline Protection	Procure Secure	CSA STAR	EuroCloud Star Audit
Risk Assessment	✓	✓	✓	
Internal Organisation	✓		✓	
Personnel	✓		✓	
SLAs and contracts	✓	✓	✓	✓
General Transparency	✓		✓	
Intellectual Property			✓	
License Issues ⁹⁵				
Third Party Audits	✓		✓	
Business Continuity	✓		✓	
Availability	✓	✓		✓
Security/ Vulnerability Management/ ISMP	✓	✓	✓	
Incident (Response) Management	✓	✓	✓	✓
Change Management		✓		
Data Center Security	✓		✓	✓
Server Security	✓		✓	✓

⁹⁵ The key issue of licensing is highlighted by the EU Cloud Strategy but not addressed by any of the four standards.

Key Issues Addressed	CSP Baseline Protection	Procure Secure	CSA STAR	EuroCloud Star Audit
Network Security	✓		✓	✓
Platform Security	✓			
Application Security	✓		✓	✓
Virtualisation/ Hypervisor Security			✓	
Data Security	✓		✓	
Multi-tenancy/ Isolation		✓	✓	
Elasticity		✓		✓
Resilience/ Back ups			✓	
Data Lifecycle Management	✓	✓	✓	
Data Protection	✓		✓	✓
Data Location			✓	
Subcontractors			✓	
Encryption	✓		✓	✓
Logging and forensics		✓	✓	
Portability/ Interoperability	✓		✓	✓
Access/ Rights Management	✓		✓	✓
Monitoring for customers	✓	✓	✓	✓
Energy efficiency				✓

5.1 Cloud Provider Certification Frameworks

5.1.1 BSI Baseline Protection

5.1.1.1 Baseline Protection and ISO/IEC 27001

The German BSI⁹⁶ (Bundesamt für Sicherheit in der Informationstechnik – English: Federal Office for Information Security; often referred to as German Information Security Agency) is the authority competent for IT security for the German federal government.

With this focus and autonomy, the BSI is internationally distinct in Europe; in the area of standardization it is comparable to the Computer Security Division of the US American NIST (National Institute of Standards and Technology).

On basis of the ISO/IEC standards 27001 and 27002 the BSI derived its detailed series of measures called BSI IT Grundschatz (BSI Baseline Protection). ISO/IEC 27001 formally specifies general requirements for a management system controlling information security and ISO/IEC 27002 contains best practices for information security management. Although these standards aim at identifying internal security risks within organizations and address them by implementing a comprehensive and coherent set of organizational and technical security measures, they do not provide a catalogue of detailed questions, which can be answered with yes or no, or measures that can be implemented straightforward.

BSI Baseline Protection bridges this gap of management standards to specific implementations by providing a catalogue of detailed measures (“safeguards”) dependent on the appropriate security level for the data and business process (normal, high, and very high). The catalog contains detailed mandatory safeguards for baseline protection (security level “normal”) and proposes some additional safeguards for more advanced security levels (“high”, “very high”). They are organized in approximately 80 modules which cover threat scenarios and safeguards for typical technical and organizational parts of an IT environment. These modules are assigned to five layers (organization, infrastructure, it systems, network, application) and cover aspects such as “hard- and software management” (layer one), “IT cabling” (layer two), “Storage systems” or “Windows Server 2003” (layer three), “System management”, “VPN” (layer four) and “Groupware”, “Active Directory”, “SAP” (layer five).

The methodology how to choose and apply safeguards is laid down in a BSI Standard (BSI 100-2)⁹⁷. For IT environments with security level “normal”, one has to choose modules (and apply the defined safeguards) according to the infrastructure, IT systems, networks and applications that are part of the IT environment. For those parts, applications and systems that are not covered by available modules (e.g., “Mac OS”, “eBanking application” or “AppStores”) or in IT environments with a higher security level (“high”, “very high”), a detailed risk analysis and development of appropriate safeguards is necessary. BSI Standard 100-3⁹⁸ provides some guidelines.

⁹⁶ https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

⁹⁷ BSI 100-2 « IT Grundschatz Methodology », , V 2.0, 2008, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile

⁹⁸ BSI 100-3 « Risk analysis based on IT Grundschatz », , V 2.5, 2008, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile

Since the baseline protection catalogue does not differentiate for different deployments of IT systems and applications, a cloud infrastructure is methodically treated the same way as an in-house data centre without virtualization, multi-tenancy or network access. As a result, the BSI baseline protection catalogue is not specifically cloud-enabling, but can be used to protect the basic IT environment. It has to be adapted and enhanced following the IT Grundschutz methodology by extending the BSI security modules to address specific processes or risks due to cloud computing.⁹⁹

5.1.1.2 Security Recommendations for Cloud Computing Providers

Especially relevant in our context of cloud computing enablers is the BSI White Paper “Security Recommendations for Cloud Computing Providers (Minimum information security requirements)”¹⁰⁰.

The BSI published a White Paper addressing at high level a multitude of issues related with the use of public and private clouds. Although the document is according to the title aimed at CSPs, it also contains lots of advice for customers. The BSI mandates a “Strategic Planning of Cloud Computing Services by Users” which supplements the necessary risk assessment of both the customer as well as the CSP because there “should always be a specific security analysis for the data or applications that are to be outsourced”.¹⁰¹ This includes specifying the protection requirements for data, applications, IT systems, cloud-services and, typically for all BSI guidelines, dividing all of these into protection requirement categories.¹⁰²

The BSI follows a risk-based approach. The White Paper does not point to specific security measures but rather describes cloud-specific risks and gives guidance on how to evaluate them and find specific countermeasures. The common IT risks addressed by BSI Baseline Protection are insufficient with regard to cloud computing. The new and cloud specific risks are derived from the well-known IT security objectives Availability, Integrity and Confidentiality.

Among several other key areas to mitigate risks the White Paper provides high-level checklists for data centre, server, network, application and data security¹⁰³ Noticeable is that the BSI does not or only in passing addresses risks in the areas of Virtualization, multi-tenancy and elasticity.

⁹⁹ One relevant extension could be the security module of IT Grundschutz covering “Virtualisation”. This has not been further analysed since it is primarily targeted at virtualisation of owned resources and therefore does not tackle many risks coming with the use of public clouds.

¹⁰⁰ BSI – White Paper “Security Recommendations for Cloud Computing Providers”, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile

¹⁰¹ BSI – White Paper “Security Recommendations for Cloud Computing Providers”, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile page 17.

¹⁰² BSI – White Paper “Security Recommendations for Cloud Computing Providers”, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile page 18.

¹⁰³ BSI – White Paper “Security Recommendations for Cloud Computing Providers”, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile page 23-33.

Additionally to security risks the BSI also touches the areas of data protection¹⁰⁴, compliance¹⁰⁵ and drawing up SLAs¹⁰⁶ and describes high-level risks in these areas. Especially valuable are the considerations on the drawing up of SLAs since the BSI clearly mandated transparency of the CSP. The CSP should give the customer information on the location of data centres, backed up by the argument that in “some countries, for example, cryptographic methods may not be used without approval. This can result in a situation where the CSP may in fact use encryption but may have to provide state agencies with access.”¹⁰⁷ Additionally, the “subcontractors crucial in delivering the cloud services must also be disclosed to customers”.¹⁰⁸

The BSI White Paper is a comprehensive foundation to evaluate potential measures the CSP wants to implement. Based on the results of this evaluation the BSI will also be able to create cloud-specific security modules. The first one named “Cloud Management” was already subject for a call for tender.

5.1.2 ENISA Procure Secure

In an effort to support institutions of the European governments with respect to procurement of cloud services, ENISA, the European Network and Information Security Agency, published a set of guidelines that outlines the parameters of secure cloud service procurement. This document, dubbed “ENISA Procure Secure”, addresses European public bodies in charge of procurement, and explains the conditions under which continuously secured cloud service procurement is feasible. Given that ENISA is responsible only for European public body institutions, the official scope of this document is restricted in that dimension, but the contents can be — and mostly are — considered almost equivalent for private sector companies that think about cloud service procurement.

The ENISA Procure Secure document consists of a set of eight “parameter groups”, each of which addresses one major field of security-related issues that may arise during cloud service procurement. Each parameter group description is accompanied with a set of topics, presented as questions to the cloud service customer, that fall into that parameter group’s domain. In total, the document asks 208 questions, each of which focuses on a specific part of one of the parameter groups.

However, the document is explicitly not trying to create some kind of certification or to present some requirements to achieve a certification. It neither tries to present criteria to

¹⁰⁴ BSI – White Paper “Security Recommendations for Cloud Computing Providers, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile page 57.

¹⁰⁵ BSI – White Paper “Security Recommendations for Cloud Computing Providers, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile page 59.

¹⁰⁶ BSI – White Paper “Security Recommendations for Cloud Computing Providers, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile page 55.

¹⁰⁷ BSI – White Paper “Security Recommendations for Cloud Computing Providers, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile page 53.

¹⁰⁸ BSI – White Paper “Security Recommendations for Cloud Computing Providers, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile page 54.

select a Cloud Service Provider, as this task is already covered in other ENISA documents.¹⁰⁹

With this paper, ENISA is going one step further, considering the case where a customer has already chosen a Cloud Service Provider. Even if the customer has followed all the criteria recommended by ENISA, it is not guaranteed that all risks are addressed on a continuous basis. Risks may change, and both the Cloud Service Provider and the customer should be able to respond to such changes at any moment.

The ENISA Procure Secure document aims to present guidelines for the implementation of continuous security controls, “*giving guidance on how to monitor the security of a cloud service on an on-going basis*”¹¹⁰.

The scope of the document covers the following aspects:

- **Security:** the parameters chosen to be covered are restricted to indicators of information security.
- **Cloud services:** although the guidelines could also be applied to other kinds of outsourced IT services, they are intended specifically for cloud procurement.
- **Public procurement:** the document focuses on the public sector, even though most of its contents apply to private sector companies equivalently.
- The ENISA Procure Secure document focuses on the service delivery phase of the life-cycle of procurement of cloud services, and advises on “how to prepare for monitoring of security-relates service levels in the contract phase”¹¹¹.

The main points of the document are:

- In order to achieve a successful adoption of cloud services, an essential part of the implementation is a security program that can cope with the specific characteristics of cloud computing and can provide the appropriate level of security to protect the customer’s information. The security management should be based on risk management and compliance. A standardized set of procedures for monitoring the security level of a cloud service, as proposed in the document, would be able to identify and assess risks in a better way.
- The procedures presented in the document are not intended to substitute other kinds of assessments, such as e.g. ISO 2700x certifications, which assure that a set of controls and procedures was in place for a certain evaluated period. The target of the ENISA procedures is to provide real time information in order to achieve security also in the intervals between other types of assessments or certification incidents.

Based on these considerations, ENISA chose eight groups of parameters to achieve a sufficient level of security monitoring. This list of eight parameters should not be understood as an exhaustive list, the parameters should always be selected according to the

¹⁰⁹ See ENISA - Cloud Computing Risk Assessment; Annex X: Contractual considerations <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment>

¹¹⁰ ENISA Procure Secure, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/at_download/fullReport p. 9

¹¹¹ ENISA Procure Secure, p. 11

organisation being monitored and its special risk areas. As ENISA explains in this document, the “*parameters should be selected according to the use-case*”¹¹². The full list consists of:

1. Service availability
2. Incident response
3. Service elasticity and load tolerance
4. Data life-cycle management
5. Technical compliance and vulnerability management
6. Change management
7. Data isolation
8. Log management and forensics

In order to make the guidelines as usable as possible for the cloud customer, each parameter is broken down as follows¹¹³:

- **Parameter definition:** What is being measured?
- **Risk profile considerations:** should I care about this parameter?
- **Monitoring and testing methodologies:** how to measure it.
- **Considerations for customer/independent testing:** how to get trustworthy measurements.
- **Thresholds:** when to raise a flag.
- **Customer responsibilities:** whose problem is it?

Based on these descriptions, European public body entities (and also private sector companies) can determine the areas of security monitoring they have to elaborate on, and if necessary can adjust in collaboration with their particular cloud service provider.

Even though this is not the primary purpose of the document, also cloud providers can use the defined parameter groups to adjust their cloud services in such a way that they support the requested degree of security monitoring, thereby enabling their cloud services to be used by European public sector entities.

In the following we provide an evaluation of the ENISA Procure Secure parameters, analysing their technical and legal implications, their particular degree of consideration of risk assessment issues, contractual issues, and monitoring issues. Finally, we conclude with an overall assessment of the ENISA procure secure guidelines, focusing on their advantages and gaps with respect to enabling privacy-aware, legally compliant, and technically secure cloud computing usage in Europe.

5.1.2.1 Service Availability

5.1.2.1.1 Technical Description

The parameter of *Service Availability* refers to the property of a certain service to be able to answer requests at any time. This includes the ability of a service requester to open a technical communication channel (e.g. a TCP connection) to the computer that hosts the

¹¹² ENISA Procure Secure, p. 11

¹¹³ ENISA Procure Secure, p. 13

service, as well as the availability and readiness of that host computer's computational resources (e.g. CPU, memory, software code etc.) to perform any requested service task.

Availability is commonly measured in percentage of time a service is responsive, such as 99.999%. Reasons for reduction of this percentage could be incidents like scheduled maintenance (and hence power-down) of the host computer, glitches or outages in the power supply, network or software failures that cause the service implementation software to crash, or lack of sufficient computational resources to execute the service instances triggered by incoming service requests. Especially the latter tends to become an issue: whenever a peak in requests for a specific service instance occurs, it is possible that the amount of requests exceeds the maximum number of service instances a host computer can execute concurrently. In that case, some of the requests must be dropped, resulting in service unavailability times, hence in a reduction of overall availability of the service. The so-called Denial-of-Service (DoS) attacks target exactly that point: by creating a huge load of service requests, these attacks try to exhaust a service's computational resources, thereby blocking the execution of valid service requests as well. If a DoS attack takes in a distributed fashion it is near to impossible to selectively ignore requests from a specific external host in order to mitigate the attack, since a multitude of computers generate this load, while each of them only issues a reasonable amount of requests that is impossible to distinguish from valid requests. The distributed hosts could stem from bot nets or even another cloud that provides the hosts at the disposal of an attacker.

One of the core promises of cloud computing is the smooth adaptation to peak loads, thereby improving on service availability percentage. Since computational resources in cloud environments commonly are huge, way larger than necessary to handle the common mean workload of a particular cloud service, it becomes possible to handle a way higher peak of service requests dynamically, as compared to a single, static, resource-constrained host computer. Furthermore, by use of virtualization, the dynamic provisioning of additional computational resources on other host computers in the same cloud becomes feasible, as virtual machine instances can be moved from one server hardware to another server hardware at runtime (so-called *migration*). Thereby, peaks in service request load can be compensated, and even scheduled downtime of server hardware can be coped with, by moving the virtual machines off of the affected hardware to other servers. In theory, this approach can lead to a service availability of 100%, however, the risk of total power outage for all server hardware in a cloud's datacentre is not negligible¹¹⁴. Hence, cloud providers usually stick to some numbers up to several digits after the decimal point.

5.1.2.1.2 Customer Risk Assessment

The ENISA questionnaire gives guidance to evaluate the potential customer's own availability requirements. The customer should identify the availability requirements of specific tasks and processes. What services, processes and data need to be accessed at a certain point in time or within a specific time frame – ongoing, daily, weekly, or less often (backups) – and how long an outage would be critical to the customer's business?

Besides varying availability requirements per process, the customer needs to think about dependencies and how other processes outside the cloud could be affected.

Example 1: A cloud customer uses a SaaS cloud for his accounting. He identifies that regularly an outage of more than one office day would be critical for his business. But in the

¹¹⁴ Cf. Amazon Web Services: Summary of the AWS Service Event in the US East Region, July 2, 2012, <http://aws.amazon.com/message/67457/> ; Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region, April 29, 2011, <http://aws.amazon.com/message/65648/>

month before the balance sheet date the availability requirements rise to a maximum outage of half an hour to fulfil his legal balancing duties in time.

Example 2: A cloud customer has identified that an outage would only become critical after two full days. This adds up to moderate availability requirements of 99.5%, which can add up to a total outage of ca. 44 hours if it occurs in one long outage rather than several small ones.

5.1.2.1.3 Contractual Considerations

Similarly to Chapter 4.1.3.5 (Contractual Enablers: Availability) ENISA points out to carefully select or negotiate the CSP's commitment to availability. It has to be evaluated if the availability rate and definition matches the customer's requirements. The availability commitment may be dependent on an outage of more than one geographical area, rely on intransparent measurements or exclude very slow response time.

The risk of a business critical outage can also be mitigated by penalty clauses.

Example 3: The cloud customer may choose a CSP that provides an uptime guarantee of 99,99% in its SLA. Alternatively, the customer may negotiate an individual contract with a CSP with varying monthly uptime guarantees. A third solution could be to use a hybrid cloud architecture to mitigate the outage risk for the balancing sheet date.

Example 4: A customer processes data that has legal restrictions on transfer outside of the EEA. He considers a globally operating CSP that offers a "European Cloud Zone" with data centres and administration in the EEA. In its SLA the CSP defines outage as a failure of at least two "Zones". Therefore, the availability guarantees of the CSP do not apply for the customer who does not agree to have his data transferred to outside of the EEA in a case of failure of the EEA zone.

5.1.2.1.4 Technical issues of monitoring and assessment

Measuring availability contains some pitfalls for cloud customers, as sheer numbers of availability percentage do not reflect the true data availability conditions of a cloud system. For instance, a 3-day cloud server outage per month (e.g. due to maintenance issues) reflects the same availability percentage value as a flickering cloud server connection that drops every 10th incoming connection. If a critical data access request falls into the 3-day outage period, the business impact for the cloud customer may be quite different from the other case, within which an instant reconnection may solve the issue within seconds.

Apart from such parameters, availability is also hard to measure in terms of localization: accessing the same set of data may vary in delay and accessibility, depending on the source of the request. For instance, accessing data on a Chinese cloud server from a cloud customer's system running in Europe may turn out to take longer than accessing that data from within China, e.g. due to Internet-scale protection architectures like the "Chinese Wall" firewall system.

Finally, measuring availability also involves a decision on whether to trust the cloud provider to collect and publish availability data, or whether the cloud customer itself (or a trustworthy third party) needs to perform external availability tests.

In terms of techniques, availability monitoring may range from testing the technical ability to connect to a cloud server (e.g. establishing a TCP connection) to downloading a full dump of all data stored at the cloud provider's site, each technique repeated in a certain period of time.

5.1.2.1.4.1 Incident Response

5.1.2.1.5 Technical Description

During operation of a data centre that hosts a cloud service, a lot of things may happen that affect the operability of these services. Considered as an incident is any event with impact on

the service that is outside of the cloud service's normal operation.¹¹⁵ Ranging from power outages to software-based attacks, from malicious manipulations by disgruntled employees to electrical or mechanical hardware malfunctions, each type of such incident may impact on the services hosted in the data centre. The parameter of *Incident Response* refers to the way to handle such incidents in a cloud environment. For instance, the type, quantity, and delay of reactions a cloud provider offers to its customers for each type of incident are relevant. These parameters may range from giving a full-disclosure documentation of a hacker attack incident, published on the cloud provider's website 5 weeks after the attack took place to almost instant distribution of automated status e-mails once a system component is affected or broken by a hardware failure. Vice versa, incidents may be detected on the side of the cloud customer, but may affect the systems of the cloud provider (e.g. a Denial-of-Service flooding attack on the cloud customer's cloud services). In that case, the parameter of *Incident Response* also covers the means (and quantities, delays etc.) of communication from cloud customer to cloud provider.

5.1.2.1.6 Customer Risk Assessment

ENISA advises the customer to evaluate the necessary time frame within which the CSP has to respond to incidents. Based on the type of incident (e.g. availability, provisioning, elasticity, logging, data breach) the requirements for the response time may vary:

Example 5: A cloud customer using a cloud service for back-up storage of their human resources data, including its employees personal data, will identify availability incidents as less severe for their business. Entirely different matters are incidents concerning data breaches or leakage. Here, the cloud customer has own legal requirements regarding e.g. breach notification. Therefore, the necessary maximum incident response time and customer notification of the CSP has to be as short as reasonably possible. In this example this could be within 6 hours after detection. Furthermore, the notification has to include detailed data about the incident regarding which data base or records are breached.

5.1.2.1.7 Contractual Considerations

If the customer has identified business critical or compliance relevant incident response times of the CSP, he may want or need to set up thresholds for several parameters. ENISA refers to the ITIL model naming: severity of the incident, time to report incidents detected by the CSP, time to respond to incidents reported by the customer, time to recovery, continued recovery reports and transparency of time since last incident.¹¹⁶

Additionally, the customer should check if the CSP has a contractual duty for notification of its customers and what this notification has to include (e.g. which customers are concerned?).

5.1.2.1.8 Technical issues of monitoring and assessment

The suitable set of monitoring techniques for the specific parameter of incident response largely depends on the type of cloud usage. For SaaS cloud environments, the cloud customer typically is hardly aware of ongoing incidents, despite some potentially detectable corruptions in its own data. Even in that case, there is no other possibility for the cloud customer than to contact the CSP (given that there is a suitable contact point for such incidents) and ask for support or status. Here, the CSP is the entity in charge for monitoring and reacting to incidents in a reasonable way.

¹¹⁵ ENISA Procure Secure, page 20.

¹¹⁶ ENISA Procure Secure, page 21.

For IaaS clouds, on the other end, the cloud customer to a large degree is responsible for incident management and response herself/himself. Since many types of incident reside on the level of operating systems or applications stacks, and since these software components in IaaS typically are operated and maintained by the cloud customer, incident response for these parts have to be operated by the cloud customer as well. The responsibilities with respect to monitoring of IaaS cloud systems are merely restricted to hardware and network issues, and to hypervisor and virtualization issues.

PaaS clouds in this sense pose a problem, since some parts of the overall software stack are operated and maintained by the cloud provider (typically involving the hardware, networks, operating system, and potentially some runtime environments), whereas the real cloud services are implemented and covered by the cloud customer. Hence, if an incident takes place in a PaaS environment, it may turn out to be hardly decidable whether the issue resides in the responsibility of the cloud provider, the cloud customer, or both. Either way, this type of cloud usage requires a large degree of collaboration between cloud provider and cloud customer, as long as incident response means are touched.

On the technical side, relevant aspects cover tamper-proof logging mechanisms of both cloud provider's services and cloud customer's services, as well as interfaces for performing forensics (e.g. creating VM snapshots), and alert contact points at both the cloud provider and the cloud customer, with reasonable terms-of-use and response delay agreements.

5.1.2.2 Service Elasticity and Load Tolerance

5.1.2.2.1 Technical Description

Being a specific part of availability regarding resource provisioning, the parameter of *Service Elasticity and Load Tolerance* covers the flexibility and scalability of hosting a particular cloud service. This involves issues of virtualization (e.g. can a virtual machine instance be moved to different server hardware? Can it be cloned multiple times?), provisioning of resources in times of high demand as well as considerations of criticality of failure of cloud services. For instance, if a particular resource or cloud service is not required by any cloud customer, it may be shut down to fend a Denial-of-Service flooding attack instead of providing additional resources to manage the huge amount of irregular service requests.

In a similar way of consideration, this parameter considers the risk and impact of demand-related failures to operate (e.g. due to an unexpected peak or drop in demand, or a Denial-of-Service attack).

Furthermore, the load tolerance aspect of this parameter refers to the common workload cycle of a cloud service. Since, commonly, most cloud services stick to a particular local area and hence a local set of time zones, it is commonly expected that service usage is undergoing a daily cycle in relation to that time zone parameter. Deviations in load may cause irregularities in the cloud hosting environment, and these irregularities have to be addressed by the cloud provider, e.g. in terms of sufficient flexibility in provisioning of computational resources, or in terms of proper load balancing means.

5.1.2.2.2 Customer Risk Assessment

The customer first needs to identify his particular elasticity requirements. Does he need a static amount of resources with constant slow growth or is his demand more volatile? If the customer identifies peaks in the fluctuation of his demand, he has to further assess if these peaks occur regularly or irregularly.

Example 6: A customer using an IaaS cloud to host his web shop for gifts identifies that 28% of his annual sales volume are made in December. This means that the number of page views and therefore the demand for resources has a regular high peak at the end of the year. Additionally DoS or DDoS attacks make it necessary to prepare for irregular volatile elasticity demand throughout the year.

Additionally, the customer needs to take into account what kinds of resources are needed for his peaks in demand: Does he need more VMs or hardware resources (e.g. bandwidth, or number and speed of CPUs)?

He also needs to consider that depending on the CSP the demand for more hardware resources can lead to slower response time or slower processing. If this is business critical for the cloud customer he needs to choose a suitable CSP accordingly.

5.1.2.2.3 Contractual Considerations

It is important for the customer to evaluate, if the CSP's SLA put restrictions or limits on the provided elasticity in times of peaks in demand. E.g. a smaller CSP could limit the access to hardware resources like bandwidth per customer for reasons of load tolerance and to protect other customers.

According to ENISA some CSPs offer a reserved guaranteed capacity independent of current demand.¹¹⁷ It is important for the contractual evaluation to identify under which circumstances this emergency capacity can be accessed (additional fee, special authentication).

Then again, a customer which has a very static demand might want to put up own restrictions for the elasticity demand of his account. To prevent a risk of high costs in case his account is compromised for resource theft, he can contractually limit the increase of elasticity demand or the amount of resources.

5.1.2.2.4 Technical issues of monitoring and assessment

Measuring elasticity and load tolerance is a highly tricky domain. Obviously, one could measure load tolerance by creating a high level of load (e.g. using flooding techniques) and monitoring the cloud service's availability and behavioural characteristics. However, this approach is not feasible in general, as especially cloud services with their elasticity means are likely not to react in a measurable way. Furthermore, performing such a test involves costs, both at the cloud provider's side and at the cloud customer's side, which may turn out to rise drastically, if the cloud elasticity means work properly. Moreover, performing those tests are likely to violate a CSP's SLA because it basically is an attack on their availability. Finally, such tests reflect only a snapshot behaviour at a given time and for a given set of cloud services and load characteristics. This does not imply a reasonable tolerance of other types of load attacks, nor a reasonable technique for continuous elasticity enforcement.

Furthermore, issues of service migration policies (when does the cloud provider replicate a service? How often? On how many servers? For what timespan?) and proper treatment of potential hardware failures have to be coped with.

On the technical side, assessing a service's elasticity characteristics without performing a load test and evaluating the reactions internal to the cloud system is hardly feasible, and is mostly an issue to be addressed by the cloud provider itself.

5.1.2.3 Data Lifecycle Management

5.1.2.3.1 Technical Description

A cloud service commonly consists of two important parts: the service implementation, and the set of running service instances. Depending on the type of cloud service, running instances may vary between short-term calculations (e.g. detecting whether a given credit card number is a valid one) and long-term provisions (e.g. storage of archived government documents). Either way, each service instance has its own set of data items attached to that

¹¹⁷ ENISA Procure Secure, page 24.

instance, and hence, such data must be stored and held available by the cloud environment for the lifetime of a service instance— – at least. Hence, the parameter of *Data Lifecycle Management* covers the handling of data items belonging to service instances within the cloud environment. How are they stored? Persistently or temporarily? Within a dedicated database on separate cloud hardware, or as part of the virtual machine instance that hosts the service implementation?

Furthermore, aspects of data archiving, back-ups, deletion and recovery are addressed in this scope. Typically, this involves technical means for data availability (e.g. by using redundancy of data storage) and integrity (e.g. by means of digital signatures, hash values, proofs of retrievability¹¹⁸, robust data deletion techniques, etc.), but also on disaster recovery issues.

5.1.2.3.2 Customer Risk Assessment

The customer has to identify or establish his process for creating back-ups of his data. This includes identifying and defining the potentially business critical process of accessing, retrieving back-ups to restore data. In which frequency back-ups are made, when can old back-ups be deleted, how much time takes it to recover data from back-ups and how much data could be lost in a worst case scenario of the back-up cycle?

The customer also has to address requirements for legal compliance. ENISA does not give guidance on the extensive data protection requirements here but mentions the special deletion requirements for personal data¹¹⁹: The customer may need to weigh his legal deletion requirements against his requirements for back-up integrity since deletion of back-up data might not always be possible. He also needs to identify his own legal duties regarding data retention and applicable retention periods.

Litigation could also pose a risk for the customer since in a cloud environment his access to forensics might be limited.

Additionally, especially in multinational clouds, governmental access to data can be an issue regarding confidentiality. If confidentiality is business critical for the customer he needs to be aware of the circumstances that allow national government agencies to access his data.

5.1.2.3.3 Contractual Considerations

To address the aforementioned risks the cloud customer has to analyse the provided SLA or negotiate with the CSP whether his retention and deletion requirements can be fulfilled. If the CSP provides an (automated) backup mechanism, the customer has to evaluate if it is necessary include this in the contract.

The contract may also include a notification commitment of the CSP regarding governmental requests for access.

If litigation and other reasons for necessary access to forensics have been identified it makes sense to negotiate with the CSP a commitment for cooperation in case the customer has a valid need of forensic data.

5.1.2.3.4 Technical issues of monitoring and assessment

Technical means to support the lifecycle of customer's data stored in the cloud involve the frequent and sufficient use of backup mechanisms, so that all data can be restored in case of total data loss or disruption. Depending on the terms of use, cloud providers do not perform

¹¹⁸ PORs: Proofs of retrievability for large files, A. Juels and B.S. Kaliski Jr. . Proceedings of the 14th ACM conference on Computer and communications security, 2007

¹¹⁹ ENISA Procure Secure, page 31.

any backup at all, or may decide not to reveal any backup data to a cloud customer. In such cases, a cloud customer may gain advantages from performing cloud backups itself.

Technically, this involves retrieval and redundant storage of all data and service implementations of the cloud customer's cloud services. For IaaS, this may involve backup of virtual machine images, along with database dumps of the core application database within the virtual machine. For PaaS, this may involve backups of the application-level implementations (e.g. application service containers, websites, or database dumps), and for SaaS, this may involve downloading a database dump of the cloud customer's data— – given that such a download service is offered by the SaaS cloud service provider.

Other critical parameters of this domain cover the period in time at which backups are performed, the security mechanisms applied to backups to prevent disruption or unintentional disclosure, and the overall management of backups (e.g. incremental storage of backup difference vectors only vs. full storage of all data at every backup period, usage of compression techniques etc.)

5.1.2.4 Technical Compliance and Vulnerability Management

5.1.2.4.1 Technical Description

Besides existing legal requirements to implement when hosting a cloud service, there are some additional types of best practice standards to consider. These are to be addressed under the scope of the *Technical Compliance and Vulnerability Management* parameter. Examples of such regulations are IT security management frameworks like ITIL, COBIT, or ISO 27001, which all put some requirements onto organizational aspects of operating IT systems in a secure way. Common requirements range from existence of proper logging and monitoring mechanisms to well-defined organizational processes to be followed in case of attacks, power outages, notifications on existing vulnerabilities or malware spreads, or other types of events that may affect the security—and hence the operability—of the IT system in consideration as a whole.

The special aspect of vulnerability management is focussed on the processes and management issues a cloud provider has to deal with when detecting— – or being notified of— – a vulnerability in its IT systems. Once the cloud provider knows about a certain vulnerability, it falls into that cloud provider's responsibility to handle this incident properly. This may involve fixing the vulnerability, but also aspects of penetration testing (was the vulnerability exploitable? What would have been the impact?), forensic analysis (Was the vulnerability actually exploited? Which parts of the system was affected? Which cloud customers were affected? How can digital evidence be taken to support subsequent legal actions? Does the cloud provider collaborate with its customers in this respect, or does he deny the vulnerability altogether?)

5.1.2.4.2 Technical issues of monitoring and assessment

Common means to measure vulnerabilities of complex software systems like cloud environments range from network-based port scanners (for detecting potential open ports) over penetration testing tools (to check whether known attack techniques can be used to exploit these open ports) to code verification techniques. Each of these can be performed to increase the number of detected vulnerabilities in a cloud system, and to trigger additional actions (like closing the vulnerability by applying a patch, closing the port, or similar means).

However, if the CSPs usage conditions do not allow a cloud customer to perform penetration tests on the cloud environment on its own, this implies that the only entity performing penetration tests on a cloud system is the CSP itself. Since the results of these penetration tests obviously are of high interest for malicious hackers, most CSPs are reluctant in terms of disclosing these vulnerability reports. On the other side, if the cloud customer is not allowed to perform network scans or penetration tests itself, and is also not allowed to investigate the

reports created by the CSP, it becomes almost impossible for the cloud customer to reasonably measure the degree of vulnerability of a cloud environment.

As with other cases, here, the type of cloud service turns out to affect the situation as well: in IaaS scenarios, most types of vulnerabilities reside on the level of application or operating system, hence must be coped with by the cloud customer. For PaaS and SaaS clouds, in contrast, most of these parts are operated and maintained by the cloud provider.

5.1.2.5 Change Management

5.1.2.5.1 Technical Description

Complex IT systems like cloud computing environments tend to evolve over time. Every new addition to the complex hardware and software stacks that were already in place implies changes to the system's parameters, ranging from additional computational resources to a higher demand for failure management capabilities. However, the implications of each such change commonly cannot be foreseen completely at time of deployment. Thus, it becomes highly relevant to the operability of a cloud environment to strictly monitor and log any changes that are applied, both to cloud hardware and cloud software. Only then it becomes possible to sufficiently investigate upcoming issues like malfunctions, and to decide whether these issues sprung from a configuration problem due to a software update, or have been part of a malicious attack incident.

The parameter of *Change Management* copes with exactly those aspects of cloud environments. Dissemination of knowledge about recent, current, or planned changes to the cloud architecture is one of the most important parameters to consider for cloud customers, and an essential part of this aspect is the cloud provider's ability— – and willingness— – to share such information sufficiently and timely with its customers.

5.1.2.5.2 Customer Risk Assessment

To properly consider change management within this risk assessment the customer has to identify in which areas changes of the CSP could have critical impact on his business or legal compliance. These are especially changes affecting the security requirements of the customer.

The legal compliance may depend on the data location. If the customer has special location requirements it would be a risk, if the CSP establishes data centres in other countries and transfers the data without notification.

5.1.2.5.3 Contractual Considerations

For this reason the most important contractual countermeasure to address change management risks is a notification obligation of the CSP. Important is that the necessary notification of relevant changes is upfront by a certain amount of time (change notice time). What relevant changes are depends on the specific case but may include changes affecting the certification status of the CSP or the customer, the applicable jurisdiction, the company ownership of the CSP, or major system changes.

5.1.2.5.4 Technical issues of monitoring and assessment

Technically, change notifications have to be communicated by a CSP in a way that allows each cloud customer to sufficiently prepare for the particular type of change. Hence, a change notification message must be pushed to the cloud customer's attention (like an e-mail), and is not sufficiently solved by means of a passive communication channel (like a post on the CSP's website or Twitter account).

Furthermore, change notifications have to be precise, complete, and conclusive. Therefore, it is reasonable for the CSP to maintain a well-structured change management process that covers all of these aspects.

Some aspects of change management have to be addressed by the cloud customer (e.g. assessing the impact of the change to the customer's cloud usage), some must be performed by the cloud provider (e.g. validating the impact of the change to certifications, policies, and operational procedures).

In each case, change notifications have to be acknowledged by the recipient (i.e. the cloud customer), and both change notification and acknowledgement should be logged.

5.1.2.6 Data Isolation

5.1.2.6.1 Technical Description

The very key aspect of cloud computing is the shared use of a pool of resources using virtualisation. Due to this sharing, isolation is an essential precondition for multi-tenancy. But the grade to which isolation is implemented and safeguarded may differ widely.

However, in terms of security, such approaches of multi-tenancy in cloud environments comes with the downside of potential leakage of information or processes from one customer's domain to the domain of another customer. Hence, the parameter of *Data Isolation* reflects this need to perform strict separation of customer domains within a cloud environment, especially with respect to data storage. Technically, this may imply providing separate storage hardware for each cloud customer, or different encryption keys being used for encryption of data from different customers. Most extreme manifestations of this approach result in separate hardware networks, or even separate data centres, for those customers that require such level of security.

A key aspect of cloud computing environments consists in the monetization of redundancy reduction. Examples make the operation of multiple cloud services on the same server hardware (saving the need for additional computation hardware), or the data compression and de-duplication techniques employed for reducing the total amount of storage required to host all customer's data (saving the need for additional storage hardware).

5.1.2.6.2 Customer Risk Assessment

For a proper Risk Assessment, the customer has to consider various states of his processes: data at rest; data in processing (RAM isolation); during transfer (network isolation); backups. A proper isolation must be provided during all of these states of the data lifecycle though the technical implementation varies.

Proper isolation also touches the issue of data deletion: is a cloud customer's wish to delete a certain data item within the cloud taken literally? If so, how is this achieved, and how can the cloud customer be convinced of this? Without proper data isolation, answering such questions may reveal information about other customers of the same cloud service (as happened for the de-duplication approach).¹²⁰

5.1.2.6.3 Contractual Considerations

The ENISA Procure Secure Document states that although CSP's have to provide isolation the customer "*rarely has visibility into the technology or configuration [...] to achieve this*".¹²¹ The document therefore makes no suggestions for contractual means but advises the customer to verify how "isolation" is defined in the SLA.

¹²⁰ Cf. Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg, "Side Channels in Cloud Services: Deduplication in Cloud Storage," IEEE Security & Privacy, vol. 8, no. 6, pp. 40-47, Nov.-Dec. 2010, doi:10.1109/MSP.2010.187.

¹²¹ ENISA – Procure Secure, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/at_download/fullReport page 43.

5.1.2.6.4 Technical issues of monitoring and assessment

Monitoring data isolation from a cloud customer's perspective involves disclosure of technical details of the internal cloud environment architecture in place at the CSP. Obviously, this touches business secrets of the CSP. Hence, most CSPs are very reluctant in this matter.

Commonly, asserting data isolation in IaaS clouds can be performed much easier than providing evidence of proper data isolation in SaaS clouds. For instance, IaaS clouds may allow for TPM-based attestation of hypervisor integrity, hence can support data isolation assessment to a large degree. For SaaS providers, however, verification of data isolation implies the necessity for the cloud customer to access and understand the internal workings of the SaaS cloud service— which is often considered a business secret of the SaaS CSP. In that case, data isolation assessment turns out to be tricky if not impossible.

5.1.2.7 Log Management and Forensics

5.1.2.7.1 Technical Description

According to some legislations, operating IT systems on behalf of other organizational entities requires the ability to perform an in-depth investigation of every type of incident arising from the IT system. Most commonly, this involves a strict, sound, and complete logging of system events in a separate log system. Access to those log files must be restricted, and are commonly only provided in the scope of a law enforcement action. However, even in that case, the log files must be shaped in a way that its log data suffices as legal evidence in court, hence must contain additional measures to safeguard data integrity and completeness. Furthermore, the existence of such log files allow for forensic analyses being performed on the events that led a cloud system into a specific situation, giving clarifications to some common types of security-related questions, e.g. whether an attack was being exploited or not.

In the scope of cloud computing, it may happen that more than one legislative domain (i.e. country) is involved in a situation of legal interest. For instance, a European cloud customer may use cloud services offered by an American cloud provider. In that case, the ability to perform forensics and log investigations largely depends on the degree of collaboration offered by the American cloud provider. Since that one is not within the domain of European laws, this may cause complications in terms of law enforcement that must be addressed prior to adoption of other-domain cloud services.

5.1.2.7.2 Customer Risk Assessment

Transparent, reliable and accessible logs may be crucial for auditing (internal and external) and liability of a customer.

To install proper logs the customer first needs to assess what needs to be logged in accordance with “internal control, compliance, and audit, legal or regulatory requirements”¹²². Furthermore, the customer needs to determine the required accuracy and reliability of the logs.

Example 7: A customer from the EU uses a SaaS cloud to process his CRM data. Since this is personal data the customer needs to comply to his national Data Protection Law transposed from the Data Protection Directive 95/46/EC. The legal requirements include among other the knowledge and evidence for the sort of data processed (no sensitive data included), what and when it has been deleted (retention periods, secure deletion), when the data has been accessed and by whom. In the case of a compliance audit or investigation by the competent DPA the customer must be able to prove his compliance. Best and

¹²² ENISA Procure Secure, page 44.

recommended practice is to give evidence via comprehensive documentation and auditable event and access logs.

Depending on the layer (IaaS, PaaS, or SaaS) the user may have to implement logs himself since he has access to the infrastructure layer or rely on the CSP to provide logs.

Another risk is the accessibility of logs for the customer. Oftentimes the CSP would not give the customer read only access to event logs or logs concerning the CSP's own data handling. The CSP might choose to provide "derived logs" which are not verifiable for the customer.

5.1.2.7.3 Contractual Considerations

The customer should evaluate or negotiate the contractual specification with regard to what exactly will be logged and in which way. Does he himself have access to the logs and are these reliable or verifiable? How the logs are kept and verified can also be a matter of contractual negotiation.

If the customer regularly only gets access to derived logs he may need to negotiate a cooperation commitment of the CSP for the case of litigation or other forensic needs.

Additionally, the customer has to verify if the availability guarantees of CSP include the availability of logs and uptime of logging services.

5.1.2.7.4 Technical issues of monitoring and assessment

Technically, a lot of solutions for tamper-evident log file generation protocols exist. Most of these are based on cryptography, mostly digital signature and hash algorithms, to attest integrity and completeness of a list of log file entries.

For the cloud computing scenario, however, these techniques pose issues of their own. For instance, if the cryptographic key used for protecting a log file of the CSP is controlled by the CSP itself, this implies the possibility of abuse, i.e. the CSP is able to alter the log file and re-apply a valid digital signature to it. Though this implies a malicious intention by the CSP (or one of its employees), it nevertheless poses another source of risk to cope with for the cloud customer.

Furthermore, completeness of log files also implies the necessity for the CSP to verifiably include all relevant events as log entries in these files. If, for instance, a CSP accesses a customer's database files directly, and decides to skip the obligatory log entry generation procedure, this implies the log file to become incomplete (since it no longer reflects *all* database accesses). Furthermore, there is no means for a cloud customer to decide whether such type of log omission has happened or not. Thus, existing log file entries can create some means of reliable information (up to the degree of legal evidence), but the existence of a secured log file does not imply (and technically cannot guarantee) its completeness.

5.1.2.8 Evaluation

This ENISA document attempts to cover the gaps / flaws in security concepts used so far. This guide is based on the information obtained from previous research done by ENISA^{123,124,125} and values the contributions made by other institutions and certification bodies (ISO¹²⁶, SSAE 16¹²⁷, ISAE 3402¹²⁸ and others).

¹²³ ENISA – Cloud Computing: Benefits, Risks and Recommendations for Information Security, <https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment>

Although the information provided by the document could be suitable for some kind of certification framework, that is not the target. The main objective is to allow continuous monitoring of the levels of security in cloud computing services, without implying that it is intended to replace other existing services in the area, for example the certification frameworks mentioned above.

This continuous control is valued as an essential objective because all ENISA reports this guide builds on have drawn the conclusion that the main models of security controls applied normally tend to make spot checks, without continuous control measures that would be required to check the security situation at a specific time or continuously. ENISA Procure Secure builds a model that can help achieve the goal of an on-going or continuous control. As mentioned above, ENISA does not aim to present an exhaustive list of security measures which should be applicable to any user of cloud computing services. The target of this guide is to raise some general guidelines to be followed. The user of this guide should keep in mind that the main goal is to find a model able to achieve the goal of the most appropriate continuous security control for its use case, and trying to use the ENISA check-list without taking care of this use case would be the wrong way of using this guide.

It should be noted that this proposal is really innovative. Most research studies and proposals for cloud security systems or guidelines for a secure migration to the cloud services are focused on the phase of Cloud Service Provider selection and in the contract phase, with special attention to the service level agreement, but virtually none, perhaps with the exception of FedRAMP continuous monitoring¹²⁹, is proposing a continuous monitoring system as proposed in this guide.

This situation is at least curious, especially if we remember the main characteristics of cloud computing architectures. ENISA, in its Cloud Computing Security Assessment report, sets the following list:

- Highly abstracted resources
- Near instant scalability and flexibility
- Near instantaneous provisioning
- Shared resources (hardware, database, memory, etc.)
- “Service on demand”, usually with “pay as you go” billing system
- Programmatic management

¹²⁴ ENISA – Cloud Computing Information Assurance Framework, 2009, <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework>

¹²⁵ ENISA – Security and Resilience in Governmental Clouds, 2011, <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector>

¹²⁶ ISO 2700x series, <http://www.27000.org>

¹²⁷ SSAE 16 Auditing Standard, 2011, <http://www.ssaе-16.com>

¹²⁸ International Standard on Assurance Engagements (ISAE) 3402, <http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf>

¹²⁹ FedRAMP continuous monitoring, http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf

At first sight, it is striking that all the above characteristics or properties have as essential virtues speed, flexibility and immediacy. These features should have a direct influence on the security measures to be applied in cloud computing services, but so far, as already discussed, there are few initiatives working in that direction. Till now, the usual way of working is to implement security measures that could be described as traditional, adapted to cloud computing as far as possible. The continuous monitoring system proposed in this paper by ENISA seems a step in the right direction by proposing proactive measures, more suitable for the field of cloud computing.

As has been described above, this guide is not trying to implement or to establish a new kind of certification, and that is the reason why this guide does not pose any prerequisites for the application of its guideline and/or check-list. The only prerequisite, if we can call it this way, is that the user decides to work with this guideline, in order to achieve a continuous monitoring of its security measures and levels, and before making this decision, the user should check if it has enough staff and technical resources for using this guideline. We must remember that, in order to achieve the goals of this guideline, the user should try to follow it as carefully as possible, and not only try to choose some questions of the check-list, answer them and write some kind of report. That could help a bit, but it would not be possible to achieve the right kind of continuous monitoring and the highest security levels achievable with Procure Secure.

Although this document does not explicitly address the main security risks in the cloud computing field, it could be helpful to make a brief reference to these risks, because this can help to understand the reasons why it could be really useful to apply the criteria presented by ENISA in this Procure Secure guide. ENISA, in its Cloud Computing Security Assessment document, mentions the following as Top security Risks in the Cloud Computing field:

- Loss of governance
- Lock-In
- Isolation failure
- Compliance risks
- Management interface compromise
- Data protection
- Insecure or incomplete data deletion
- Malicious insider

A brief look at this list makes clear that it could be extremely complicated, and risky, to give the whole control of these risks to a certification obtained at a given time and which only establishes later controls after a long period of time, or to a security system which does not pose the most continuous possible revisions of security levels.

Although the document focuses in the public sector, all the criteria presented are applicable to the private sector. Possible differences could be caused by the type of information processed, which would involve different security measures and therefore different needs to control the security levels which should be achieved with these measures.

This guideline does not focus on privacy as a main goal, but by its applying it could be possible to achieve some Privacy benefits.

The Article 29 Working Party, in its WP 196 about cloud computing¹³⁰, remembers that “Article 17(2) of Directive 95/46/EC puts full responsibility on cloud clients (acting as data controllers) to choose cloud providers that implement adequate technical and organisational security measures to protect personal data and to be able to demonstrate accountability. In addition to the core security objectives of availability, confidentiality and integrity, attention must also be drawn to the complementary data protection goals of transparency, isolation, intervenability, accountability and portability”.

Reviewing the parameters chosen by ENISA and the raised checklist, it seems clear that improvements regarding privacy can be obtained applying the guidelines outlined in Procure Secure careful, affecting the core security objectives and transparency as well.

5.1.3 CSA STAR, CAIQ, and the Cloud Controls Matrix

In its effort to foster a more standardized treatment of cloud security aspects, the Cloud Security Alliance¹³¹ provides and maintains a set of semi-formalized, publicly accessible specifications that can be used to describe and assess industry best practices and common security requirements w.r.t. security, trust, privacy, compliance, and similar aspects of cloud computing environments.

One of these initiatives, the **Governance, Risk Management and Compliance (GRC) stack**¹³², provides guidelines for a detailed assessment of a cloud provider’s systems. This can be performed according to one of the four specifications of the GRC stack, which are:

- CloudAudit (formerly known as “API for Automated Audit, Assertion, Assessment, and Assurance (A6)” of cloud providers),
- Cloud Controls Matrix (CCM),
- Consensus Assessments Initiative Questionnaire (CAIQ), and
- Cloud Trust Protocol (CTP).

Out of these, the Cloud Controls Matrix and Consensus Assessments Initiative Questionnaire specifications are the most relevant.

5.1.3.1 Cloud Controls Matrix (CCM)

The **Cloud Controls Matrix**¹³³ in version 1.2 consists of a list of 11 so-called *Control Areas*, namely

- Compliance,
- Data Governance,
- Facility Security,

¹³⁰ Article 29 Working Party, WP196, Opinion 05/2012 on Cloud Computing, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

¹³¹ Cloud Security Alliance, <https://cloudsecurityalliance.org/>

¹³² Cloud Security Alliance GRC Stack: Governance, Risk Management and Compliance, <https://cloudsecurityalliance.org/research/grc-stack/>

¹³³ Cloud Security Alliance Cloud Controls Matrix (CCM) V1.2, https://cloudsecurityalliance.org/research/ccm/#_version1_2

- Human Resources Security,
- Information Security,
- Legal,
 - Operations Management,
 - Risk Management,
 - Release Management,
 - Resiliency, and
 - Security Architecture.

Each of these has a specific set of sub-properties, defining aspects of the particular domain. In total, there are 100 such properties, with the control areas of *Information Security* and *Security Architecture* containing the dominant chunks of these. To give an example of such properties, the control area of *Information Security* lists the specific properties of *encryption (IS-18)*, *user access restriction/authorization (IS-08)*, and *segregation of duties (IS-15)*.

For each property of each control area, the Cloud Controls Matrix lists that property's applicability and relevance in the various manifestations of cloud systems. These are categorized by their aspects in the following domains:

- Architectural Relevance (Physical, Network, Compute, Storage, Application, Data),
- Corp Gov Relevance,
- Cloud Service Delivery Model Applicability (SaaS, PaaS, IaaS),
- Supplier Relationship (Service Provider, Tenant/Consumer), and
- Applicability in the scope of some common certification schemes (namely COBIT 4.1, HIPAA / HITECH Act, ISO/IEC 27001-2005, NIST SP800-53 R3, FedRAMP, PCI DSS v2.0, BITS Shared Assessments SIG v6.0, BITS Shared Assessments AUP v5.0, GAPP, Jericho Forum, and NERC CIP).

Based on this matrix, an observer can easily determine which of the given properties apply to a specific cloud providing scenario, and to which requirements within each of the given certification schemes a property may correlate.

5.1.3.2 Consensus Assessments Initiative Questionnaire (CAIQ)

Derived from the Cloud Controls Matrix, the **Consensus Assessments Initiative Questionnaire**¹³⁴ in version 1.1 provides a list of 196 questions, dealing with aspects from all control areas and sub-properties. Each of these questions can be answered with just “yes” or “no”, but may also act as a starting point for onward interrogations within the process of assessing a cloud provider's cloud security conditions. An example for such a question for

¹³⁴ Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ), <https://cloudsecurityalliance.org/research/cai/>

the specific property of *encryption (IS-18)* would e.g. be “Do you have a capability to allow creation of unique encryption keys per tenant?”¹³⁵ (IS-18.1).

Again, as with the Cloud Controls Matrix, the Consensus Assessments Initiative Questionnaire lists the corresponding requirements from each of the certification schemes given in the Cloud Controls Matrix for each of the questions provided.

5.1.3.3 The CSA Security, Trust, and Assurance Registry (CSA STAR)

Along with the CCM and CAIQ self-assessment scheme for cloud providers, the CSA also hosts a public registry that allows cloud providers to provide their completed CAIQ or CCM description to potential cloud users. This registry is called **CSA Security, Trust & Assurance Registry**¹³⁶, and started operation in late 2011. As of writing, the registry lists 14 entries¹³⁷, containing some prominent cloud providers like Amazon AWS¹³⁸, Microsoft Windows Azure¹³⁹, Telecom Italia¹⁴⁰, or Terremark¹⁴¹.

Though the initial intent of the CSA STAR registry seems to have been the publication of the completed CAIQ forms of registry applicants, the existing registry entries mingle CAIQ forms with extended versions of the CCM spreadsheet. More specifically, instead of answering each of the CAIQ questions with “yes” or “no” solely, most registrants chose to extend that answer with some remarks, sometimes even omitting a dedicated “yes” or “no” completely. Some registrants even stepped back to answering a whole block of questions (or even a whole CCM control area) with a full-text paragraph related to the particular domain of interest—but without precisely stating a “yes/no” answer to the individual questions of that control area. This could be beneficiary for potential customers since a binary yes/no answer would not allow for a comprehensive comparison of CSPs.

In August 2012 the CSA announced cooperation with the British Standards Institution to extend the STAR Registry to create a global certification scheme for CSPs. The CSA has outlined the three levels of its open certification framework:¹⁴²

1. **CSA STAR Self-Assessment:** In this first level of certification, cloud providers can submit reports to the CSA STAR Registry to indicate their compliance with CSA best practices. This is available now.
2. **CSA STAR Certification:** At the second level, cloud providers require a third-party independent assessment. The certification leverages the requirements of the ISO/IEC 27001:2005 management systems standard together with the CSA Cloud Controls Matrix (CCM). These assessments will be conducted by approved certification bodies only. It will be available sometime in the first half of 2013.

¹³⁵ Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ) V1.1, F86 https://cloudsecurityalliance.org/wp-content/uploads/2011/03/CSA-CAI-Question-Set-v1-1_FINAL_v6.xlsx

¹³⁶ Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR), <https://cloudsecurityalliance.org/research/initiatives/star-registry/>

¹³⁷ Cloud Security Alliance, STAR Registry Entries, <https://cloudsecurityalliance.org/research/initiatives/star-registry/>

¹³⁸ Amazon Web Services (AWS), <https://aws.amazon.com/>

¹³⁹ Microsoft Windows Azure, <http://www.windowsazure.com/>

¹⁴⁰ Telecom Italia S.p.a. Hosting Evoluto, <http://www.telecomitalia.com/>

¹⁴¹ Terremark, <http://www.terremark.com/>

¹⁴² CSA – Open Certification Framework, <https://cloudsecurityalliance.org/research/ocf/>

3. The STAR Certification will be enhanced in the future by continuous monitoring-based certification. This certification is still undergoing development.

As of today, only the CSA STAR Self-Assessment has been published but a cloud certification framework with the broad support of the CSA and its members seems very promising.

5.1.4 EuroCloud and the SaaS Star Audit

EuroCloud¹⁴³ is an independent non-profit organization that is made up by local chapters among many European countries. It intends to foster the adoption of the Cloud Computing paradigm throughout society, and to take an active role in the design of cloud industry processes and standards. One of the EuroCloud members, the local chapter of Germany named EuroCloud Deutschland_eco e.V.¹⁴⁴, also maintains a cloud provider certification scheme. In some publications, it is named the **EuroCloud Star Audit**¹⁴⁵, other sources list the certification as “EuroCloud SaaS Gütesiegel”¹⁴⁶. Either way, the certification scheme itself consists of a set of roughly 200 questions, which initially have to be answered by certification applicants. Then, after verification of the applicant’s answers, EuroCloud reserves the right to perform additional verifications, including an on-site audit visitation, and in case of successful verification provides an official certification. The EuroCloud Star Audit certification has five different levels (*SaaS Stars*), with level 5 being the highest level, and is awarded for a 2-year period.

The questionnaire used as a basis for the EuroCloud Star Audit is not publicly available, however, it is claimed¹⁴⁷ to cover the following aspects (depending on the requested SaaS Star level):

- Contract & compliance
- Operations & infrastructure
- Application
- Implementation
- On-Site Audit validations
- Security
- Management Processes

Examples of requirements validated in these scopes are:

- Validation of contractual clauses

¹⁴³ EuroCloud Europe, <http://www.eurocloud.org/>

¹⁴⁴ EuroCloud Deutschland_eco e.V., <http://www.eurocloud.de/>

¹⁴⁵ EuroCloud Star Audit, EuroCloud Deutschland_eco e.V., <http://www.saas-audit.de/>

¹⁴⁶ Andreas Weiss: *Cloud Computing und SaaS - Transparenz und Sicherheit durch das EuroCloud SaaS Gütesiegel*, 2. EuroCloud Workshop SaaS Gütesiegel, Feb. 2010, http://www.eurocloud.de/files/2010/04/100428_Weiss_EuroCloud.pdf

¹⁴⁷ Cf. EuroCloud Deutschland_eco e.V.: *Leitfaden Cloud Computing Recht, Datenschutz & Compliance*, and <http://www.saas-audit.de/426/anforderungen/>

- Validation of the provided level of support
- Analysis of VPN infrastructure (if present)
- Validation of energy efficiency
- Validation of support forums
- Validation of the pricing model

As can be seen, the scope of the EuroCloud Star Audit certification scheme is far more oriented towards economic aspects and business reliability, as compared to e.g. the CSA STAR¹⁴⁸ certification.

It is difficult to provide an assessment for the EuroCloud Star Audit since there is too few information available. It seems dubious that the certification scheme does differentiate five levels of compliance; one up to five stars. Basic requirements like data centre security or review of SLAs come only with a higher ranking of “star audit”. The certification levels of one star, two stars and three stars appear incomplete and therefore not particularly meaningful in choosing a cloud provider. The four and five star audits appear to be more auspicious, though due to the lack of detailed information about the certification criteria and process this cannot be conclusively determined.

5.2 Privacy-Enhancing Approaches for Commodity Clouds

5.2.1 Anonymization and Pseudonymization

On the technical side of achieving privacy law compliance when using cloud computing resources, one of the most simple yet most effective approaches consists in data minimization. If the cloud user does not transfer personal information to the cloud provider at any time, there is no risk of eventual disclosure of private information at the side of the cloud provider. Hence, if that constraint is followed precisely throughout all interactions among cloud users and cloud providers, the resulting system becomes more privacy friendly implicitly.

However, the crux of this approach is that almost every type of data can become personal information in some context. For cloud contexts, even the timing information from user-to-cloud interactions must be considered as personal information (since they disclose an individual’s capability to access the Internet, office hours, productivity of employees and often also allows for coarse-grained location queries).

In order to overcome this problem, the two approaches of **anonymization** and **pseudonymization** can be applied. Anonymization cuts off the link of a particular data item to the individual completely, the data is altered in a way so the comprised information cannot be referenced to an identified or identifiable natural person anymore. Technically, anonymity of a subject means that the subject can not be uniquely characterised within a set of all possible subjects, the anonymity set¹⁴⁹. In contrast to pseudonymisation anonymisation is

¹⁴⁸ Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR), <https://cloudsecurityalliance.org/research/initiatives/star-registry/>

¹⁴⁹ Pfitzmann/Hansen, *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, p. 9.

irreversible. The problem with anonymized data is that it loses much of its information value. Anonymized data can only be used for statistical purposes. Since it is not linked to an individual anymore it is not considered personal data. Hence, data protection laws do not apply.

Pseudonymization masks the connection between an information item and its owning individual in such a way that the connection cannot be resolved without additional knowledge, namely the mapping between pseudonyms. The quality of pseudonymisation can vary significantly. It can range from complete databases, where only the name as a direct identifier has been replaced (e.g. a database of clients – after replacing the name each customer could still be identified based on address and phonenumber) to distributed databases that must be combined to gain comprehensive information about one individual. Hence, pseudonymisation as a data security measure in the sense of Art. 17 Data Protection Directive 95/46/EC has to be evaluated on a case-by-case basis.

Problematic in the context of cloud computing and big data is that (falsely considered) anonymized and pseudonymized data can be aggregated and linked to identifying profiles again. Therefore, unlinkability should always be a protection goal to measure processes.

5.2.2 Encryption and Digital Signatures

One of the most commonly used approaches to technically guarantee specific security conditions is the application of algorithms from the mathematic discipline of cryptography. Each of these algorithms is designed such that its application provably sticks to specific conditions, which results in formally provable guarantees that specific types of events cannot happen.

Among the large set of cryptographic algorithms, two major domains have evolved to most common practical use: encryption and digital signatures.

The use of **encryption** enables a data owner to perform some transition on an arbitrary data item, mapping it from its plain text appearance to some ciphertext appearance (*encryption*) and vice versa (*decryption*). Depending on the cryptographic algorithm used, these two tasks involve one or two additional data items, the cryptographic keys. Without the correct key required for a specific encryption or decryption task, nobody can perform that encryption or decryption, respectively.

For the specific case of **symmetric encryption**, the cryptographic key used for encryption and decryption are identical; they have to be kept secret among all authorized parties. If that key happens to be disclosed, all encrypted data is threatened by disclosure as well. In the specific context of cloud computing, a common application of symmetric encryption consists in encrypting all files prior to storing them in the cloud, and decrypting them on demand after downloading back from the cloud. A key requirement here is that the cloud provider never learns about the encryption keys used. If that assumption holds, it can be proven that the cloud provider is unable to learn about the contents of the files it stores.

For **asymmetric encryption** schemes, the keys used for encryption and decryption differ. Whereas everyone can perform the encryption of arbitrary data (since the encryption key is publicly available), the specific key used for decryption is kept secret by its owners, resulting in the condition that only authorized entities gain access to the plaintext of any encrypted data— unless the decryption key gets disclosed. In the field of cloud computing, asymmetric encryption could be used similarly to symmetric encryption, however, due to its lousier performance, symmetric encryption is commonly preferred. Typical applications of asymmetric encryption schemes deal with tasks of management for symmetric encryption keys, e.g. for distribution among a specific set of authorized entities (that can perform the decryption of the asymmetrically encrypted symmetric key values).

The second major domain of application of cryptology consists of various types of **digital signatures**. As with encryption, these algorithms guarantee a certain condition with respect to an arbitrary piece of input data. Here, the guarantee asserts the property that a specific piece of data was created by someone in possession of the private key, hence the authenticity can be guaranteed. These digital signature schemes often have the positive side-effect of detecting manipulation, because the verification of the digital signature fails when it was tampered with.

As with encryption, the use of digital signatures consists of two tasks, which are *signature application* and *signature verification*. Again, each task requires a cryptographic key, which is again restricted in that it may only be disclosed to entities allowed to perform one of the tasks. Commonly, the cryptographic key used for signature application is to be kept secret, and allows for identification of the entity that applies a digital signature to the particular piece of data. The key used for signature verification, however, is mostly distributed arbitrarily (sometimes even as part of the digital signature itself), and can be used by any entity that wants to verify a digital signature's validity and origin. In the domain of cloud computing, applying a digital signature to all files prior to uploading them to the cloud enables a cloud user to later on verify their authenticity. If only integrity requirements are needed, symmetric schemes such as Message Authentication Codes (MAC) are commonplace. They use a symmetric key that the creator keeps private to attach the MAC to data. Later, using the given data, the attached MAC and the private symmetric key, the integrity of that data can be verified. If the key were disclosed, the cloud provider could perform a valid signature application or MAC creation task on the data in question, allowing him to obfuscate all types of changes he may perform.

In legal terms, state of the art encryption of data with adequate key management is one of the most effective means to safeguard privacy and confidentiality when outsourcing data to a cloud service provider. Nevertheless, at least in the European Union encryption is not considered to relieve the responsible cloud customer from the legal obligations.¹⁵⁰ Encrypted data keeps the nature it has in its decrypted state; encrypted personally identifiable information is still personally identifiable information.¹⁵¹ Encryption is considered an important technical security measure; however, additional mandatory legal safeguards still apply. For personally identifiable data this means that e.g. adequate contracts for the export of data outside of the European Economic Area have to be in place.

5.2.3 Usage of Multiple Cloud Environments

On the technical side of the cloud computing paradigm, multiple architectural approaches exist that potentially lead to improved security or privacy features. Commonly, many of these approaches are based on the existence of more than one cloud provider, and exploit this condition to gain some advantages w.r.t. security or privacy. In the following, we discuss the most prominent types of such „multi-cloud“ approaches (see *Jensen et al.*¹⁵² for a survey), and analyze their capabilities and restrictions in terms of legal obligations for cloud users and providers.

¹⁵⁰ Please refer to chapter 4.1.2.10 and 4.1.3.4 for further information.

¹⁵¹ Article 29 Working Party, WP 196, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf page 15.

¹⁵² Meiko Jensen, Jörg Schwenk, Jens-Matthias Bohli, Nils Gruschka, and Luigi Lo Iacono: *Security Prospects through Cloud Computing by Adopting Multiple Clouds*. Fourth IEEE International Conference on Cloud Computing, Washington, D.C., U.S.A, pp. 565-572, 2011.

5.2.3.1 Global Legal Considerations on Utilizing Multiple Cloud Providers

Since legislation traditionally only slowly copes with technological paradigm shifts, there are few to none cloud specific regulations in place by now. Therefore, for cloud computing the same legal framework is applicable as for any other means of data processing. Generally, legal compliance does not distinguish between different means of technology but rather different types of information. For instance, enterprises are facing other legal requirements for the lawful processing of their tax information than for the lawful processing of their Customer Relationship Management. A one-cloud-fits-all approach does not reflect these differing compliance requirements.

Multi-cloud architectures may be a viable solution for enterprises to address these compliance issues. Hence, this section gives a coarse-grained legal analysis on the different approaches, and their flaws and benefits in terms of compliance and privacy impact.

The immanent conflict between cloud computing and the world of laws and policies stems from the borderless nature of clouds, in contrast to the mostly national scope of legal frameworks. The most successful cloud service providers operate their clouds across national borders in multiple data centres all over the globe. Hence, they can offer high availability even in case of regional failure as well as reduced costs because of their choice of location. In contrast, the cloud customer is subject to its national legal requirements, and faces the problem to ensure legal compliance to national laws in a multinational environment. This conflict is neither new nor unique to cloud computing, but the highly dynamic and virtualized nature of clouds intensifies it as the applicability of laws relate to physical location.

The legal uncertainties of cloud computing, especially in Europe with its strict data protection laws, are subject to an ongoing discussion. Nevertheless, legal experts agree that lawful cloud computing is possible as long as the adequate technical, organisational and contractual safeguards for the specific type of information to be processed are in place.

Usually, enterprises process varying types of information, which have different grades of sensitivity and need according security controls. There may be business-critical information, which requires maximum availability, but is less critical in terms of confidentiality. Similarly, there may be information for which a guaranteed availability rate of 99% is sufficient, but a breach of confidentiality would be crucial. Legal and other compliance frameworks may ask for specific additional safeguards. Cloud customers based in the European Union that are contracting with cloud service providers inside or outside the European Economic Area to outsource the processing of personal identifiable information have to adhere to the EU Data Protection Directive 95/46/EC. This includes mandatory contractual safeguards for the export of personal data, such as Standard Contractual Clauses and (Processor) Binding Corporate Rules¹⁵³. Furthermore, many national legislations require specific information to stay within the national borders of the country. This typically applies to information regarding national security, but also to information of public authorities or electronic health records.

For U.S. based cloud customers several standards might be relevant: For instance, for processing of medical information of U.S. citizens, a HIPAA¹⁵⁴ certification may be required. Similarly, for credit card information processing, compliance to the PCI DSS¹⁵⁵ is mandatory.

¹⁵³ Please refer to chapter 4.2.

¹⁵⁴ Health Insurance Portability and Accountability Act of 1996, <http://www.gpo.gov/fdsys/search/pagedetails.action?granuleId=CRPT-104hrpt736&packageId=CRPT-104hrpt736>

¹⁵⁵ Payment Card Industry Data Security Standard, https://www.pcisecuritystandards.org/security_standards/index.php

Further, FISMA¹⁵⁶ and FedRAMP¹⁵⁷ are relevant for processing information of U.S. Federal Agencies.

Potential cloud customers are facing several of these requirements for security controls, standards and certifications, probably even varying per process. Identifying one cloud service provider to offer all of these options like a modular system seems impossible.

Multi-cloud approaches may help addressing these issues. The compliance benefits and drawbacks of the identified multi-cloud architectures in general seem auspicious.

5.2.3.2 Knowledge Splitting Approaches

The first and most obvious approach of using multiple clouds to gain (perceived) security improvements consist in distributing the data or applications of the cloud user among all cloud providers. This can be done in several different ways, each of which is analyzed in the following subsections. Note that, obviously, it is also possible for a cloud user to utilize a combination of two or more of these approaches, trying to gain the combined benefits from all of these. Though this is technically feasible, we identified most combinations to not have a major influence on the legal considerations and obligations of the resulting cloud systems. However, if exceptions to this observation exist, they are discussed at the particular approaches' subsections in detail.

5.2.3.2.1 Plain Redundancy („Replication of Data/Application“)

This straight-forward approach of using multiple cloud providers to gain advantages on the security side simply repeats all processes of the cloud user on each of the involved cloud providers. If the cloud service is data storage, this implies all data of the cloud user is being stored on all cloud providers. Hence, every cloud provider holds a full copy of all data of the cloud user.

If the cloud service consists in providing a particular service, such as execution of virtual machine instances or realization of particularly purposed business workflows, this approach is commonly implemented by having the same workflow, VM instance, service etc. being deployed on each cloud provider's systems, and running the same calculations on each of these concurrently. Hence, obviously, each cloud provider has full knowledge and full control over all executions within its site.

¹⁵⁶ U.S. Federal Information Security Management Act of 2002, <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

¹⁵⁷ U.S. Federal Risk and Authorization Management Program, <http://www.gsa.gov/portal/category/102371>

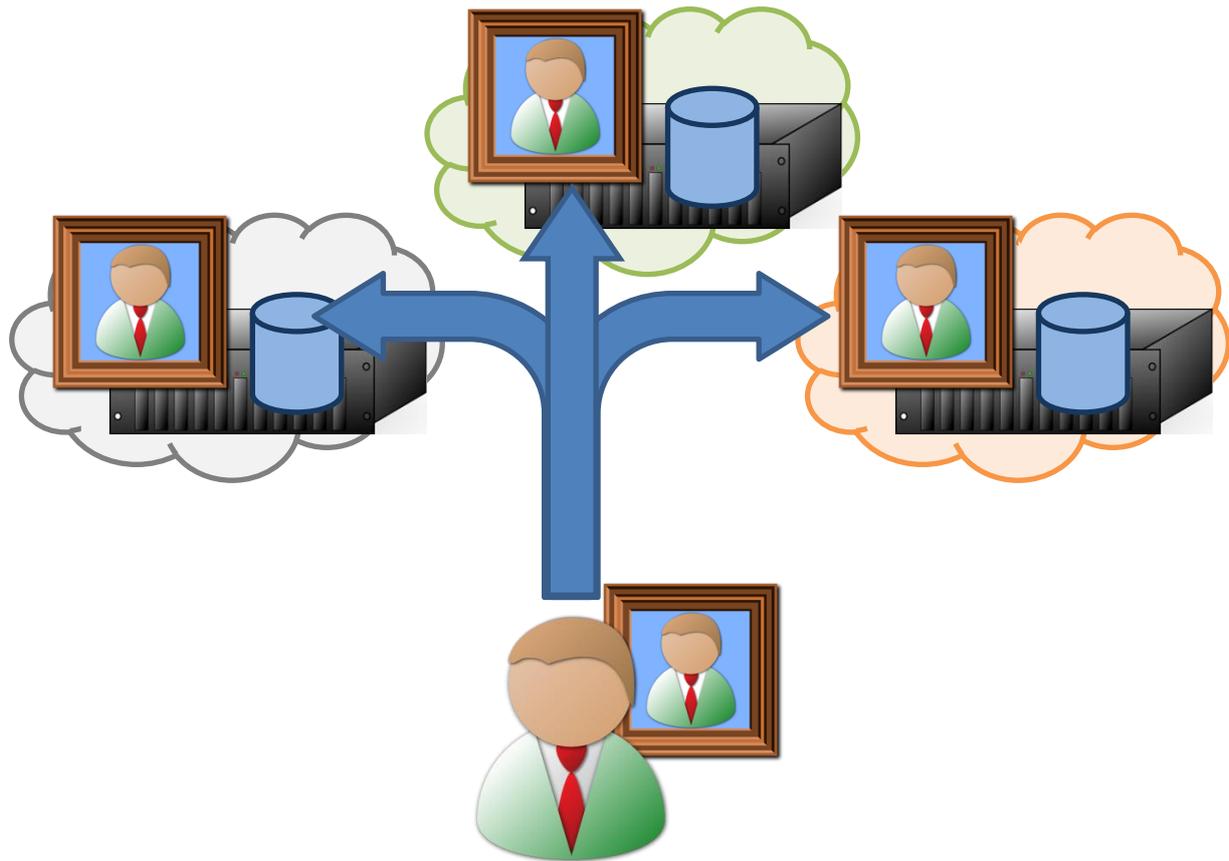


Figure 3: Replication of data by using multiple clouds

The benefit of utilizing this redundancy-driven multi-cloud approach is trivial: by comparing the data, or the results of service executions, respectively, retrieved from all of the involved cloud providers, a cloud user can easily determine that the data/calculation result exists (*availability*) and is identical (*integrity*) for all cloud providers. This prevents cloud providers — and external adversaries — from maliciously tampering with data or process executions, and allows the cloud user to gain a higher level of trust into the cloud system with regard to data availability and integrity. Moreover, this approach clearly improves availability and resilience of data and processes.

This approach appears to have few benefits regarding legal compliance as it multiplies the necessity to identify and choose a cloud service provider perfectly tailored for the requirements of the relevant process and information. Since this could mean negotiating and concluding individual contracts with several cloud service providers, replicating a highly sensitive process or an application seems to unreasonably tie up personnel and financial resources. Therefore, this approach has its value for information and processes with low sensitivity but high availability and soundness requirements.

5.2.3.2.2 Data Splitting

Instead of utilizing multiple cloud providers for gaining data integrity, a complementary approach of data splitting consists in storing only a fragment of the total data of the cloud user on each cloud provider's site. Thus, for this approach the cloud user splits its total set of data into n fragments, and distributes these fragments among the n cloud providers. As a result, each single cloud provider can only see a fraction of the total data. Furthermore, only the cloud user can reconstruct the complete dataset, by pulling all data from all n cloud providers together.

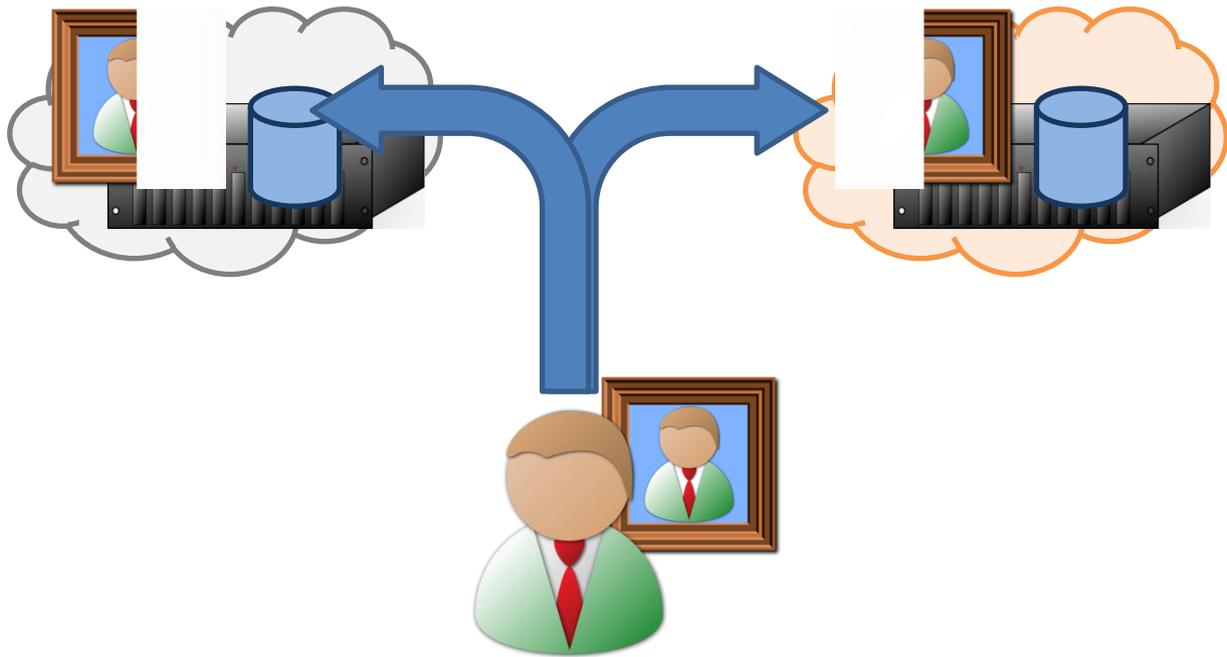


Figure 4: Data splitting approach using two clouds

The advantage of this architecture is that none of the cloud providers can see the full dataset. Thus, the cloud user is able to hide some aspects of the complete data, such as the total size of the dataset (as long as the cloud providers do not learn the value of n and the average size of the data fragments). Furthermore, a single cloud provider is not able to tell whether a specific data item is contained within the overall dataset, unless it happens to be present exactly in its chunk of the total data. Hence, in one n -th of all cases, a cloud provider can definitely tell the data item to be present, and in all other cases is not able to tell whether it is contained in the overall dataset or not. This is often considered as a benefit in terms of data disclosure (*confidentiality*).

The separation of logic and data offers the possibility to store the data in the cloud with compliant controls and safeguards and to outsource the processing logic to a not specifically certified cloud with favorable price. It also allows for storing the data in a national cloud while the application logic is outsourced to a multinational one.

These approaches are especially valuable for dealing with personal identifiable data. Segmenting personal identifiable data— – if realized in a reasonable way— – is a viable privacy safeguard. Best practice would be to separate the data in a way that renders the remaining data pseudonymous. Pseudonymity itself is a privacy safeguard. Therefore, outsourcing pseudonymized information which is unlinkable to a specific person does require considerable less additional safeguards as compared to non-pseudonymized information.

Pseudonymization based on the Obfuscated Splitting approach could be used e.g. in Human Resources or Customer Relationship Management. A potential cloud customer would have to remove all directly identifying data in the first place, like name, social security number, credit card information, or address, and store this information separately, either on premise or in a cloud with adequately high security controls. The remaining data can still be linked to the directly identifying data by means of an unobvious identifier (the *pseudonym*), which is unusable for any malicious third parties. The unlinkability of the combined pseudonymized data to a person can be ensured by performing a carefully conducted privacy risk assessment. These assessments are always constrained by the assumptions of an adversary's "reasonable means". The cloud customer has the option to outsource the pseudonymized data to a cloud service provider with fewer security controls, which may

result in additional cost savings. If the customer decides to outsource the directly identifiable data to a different cloud service provider, she has to ensure that these two providers do not cooperate, e.g. by using the same IaaS provider in the backend.

5.2.3.2.3 Process Splitting

Similar to the previous one, the approach of process splitting is used to hide some details about an overall process execution from the cloud providers. Again, initially, the cloud user has to fragment the overall process intended to be executed in a multi-cloud environment into chunks, and distribute each such chunk to a different cloud provider. This requires a slight modification to the overall process, since every chunk has to be completed with a data input interface (used by the provider of the previous chunk of the same process) and a data output interface (where the intermediate results of a chunk execution are propagated to the next cloud provider). Hence, once the cloud user has connected all chunks to form an appropriate line of execution, the overall process is implemented in a way that none of the cloud providers can see the full process (*confidentiality*), but in total, the cloud user is provided with the full result of the overall process calculations.

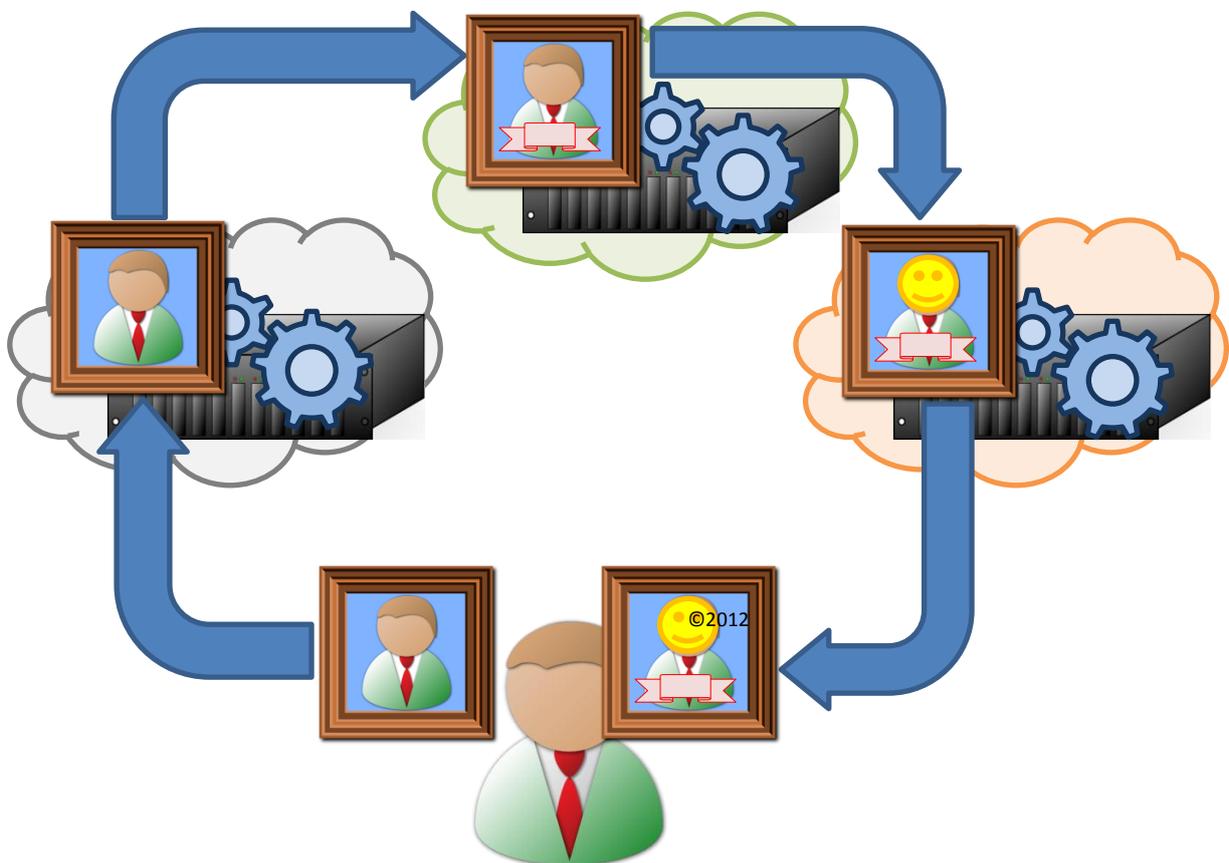


Figure 5: Process splitting by using multiple clouds

Obviously, this approach of process splitting is not always feasible. For instance, it may be doubted whether the execution of a virtual machine instance can be “split” reasonably so that it is provided by more than one cloud environment. However, the approach may work fine if the process e.g. deals with rendering video data, tax calculations, or common business process executions.

A remarkable aspect of this approach of process splitting is that it may be used in conjunction with the data splitting approach in a convenient way: each chunk of the overall

process is provided with exactly that part of the overall data that it requires for its purpose, via the data input interface. Thus, it is not necessary to provide access to the full dataset underlying the process execution, and hence, each cloud provider can only learn about that fragment of the overall data that happens to be processed in the chunks located at its cloud environment.

As of today, a combined approach of data and process splitting appears to be the most viable alternative, both from the technical and economical point of view. Domain splitting is already adopted by cloud customers in community clouds that deal with easily separable processes. However, standardized protocols and interfaces for different clouds to seamlessly interact are missing. This issue usually prevents the application of this approach to more complex scenarios in practice.

5.2.3.3 Hybrid Clouds, and InterClouds

One of the often-stated arguments for cloud adoption is the promise of almost infinite computational resources, along with on-demand scalability. Obviously, though public cloud providers commonly maintain several huge data centres with high-performance server racks, the resource capacity of every cloud is limited. Hence, especially for non-public clouds, e.g. for private in-house clouds of an enterprise, it may happen that the available computational resources are not sufficient to cope with an ongoing peak in workload. In that case, one approach consists in outsourcing some of that peak workload to a different cloud provider's systems on-the-fly. For instance, if the number of virtual machine instances concurrently running in one cloud environment reaches its capacity limit, it is feasible – and reasonable – to migrate some of these virtual machine instances dynamically to a different cloud provider, one with existing free computational resources.

Hybrid Clouds is the term regularly used for a combination of private and public cloud.¹⁵⁸ The assumption here is that both a private and a public cloud exist, which are transparently used in conjunction such that the cloud user is not bothered to deal with the details. The most common realization of that type of multi-cloud is the scenario of a private cloud which outsources to a public commodity cloud whenever the computational resources of the private cloud are exhausted.

Depending on the deployment a hybrid cloud allows the customer to separate its data and processes according to sensitivity.

*InterCloud*¹⁵⁹ refers to a quite similar approach, with the slight difference that it is commonly used for mutual interaction among public clouds (or private clouds), so there is no private-to-

¹⁵⁸ NIST has a broader definition of Hybrid cloud including all cloud deployment models, The NIST Definition of Cloud Computing, <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> page 3

¹⁵⁹ Kevin Kelly: *A Cloudbook for the Cloud*, 2007, http://www.kk.org/thetechnium/archives/2007/11/a_cloudbook_for.php;

David Bernstein, Erik Ludvigson, Krishna Sankar, Steve Diamond, and Monique Morrow: *Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability*. 2009 Fourth International Conference on Internet and Web Applications and Services, Venice, Italy, pp. 328-336, 2009;

Antonio Celesti, Francesco Tusa, Massimo Villari, and Antonio Puliafito: *Security and Cloud Computing: InterCloud Identity Management Infrastructure*. Seventh International Workshop on Emerging Technologies for Next Generation GRID (ETNGRID), Larissa, Greece, pp. 263-265, 2010;

Rajkumar Buyya, Rajiv Ranjan, and Rodrigo N. Calheiros: *InterCloud: utility-oriented federation of cloud computing environments for scaling of application services*. In Proceedings of the 10th international conference on Algorithms and Architectures for Parallel Processing, Busan, Korea, pp. 13-31, 2010.

public consideration beneath. Moreover, in one shape, the InterCloud approach does not require full collaboration between the two cloud providers; the migration target of the InterCloud approach does not necessarily have to be aware that the workload delivered by the source cloud actually belongs to a cloud environment.

The InterCloud follows the same direction as the TClouds Cloud-of-Clouds approach, offering great benefits in resilience, fault-tolerance and elasticity.

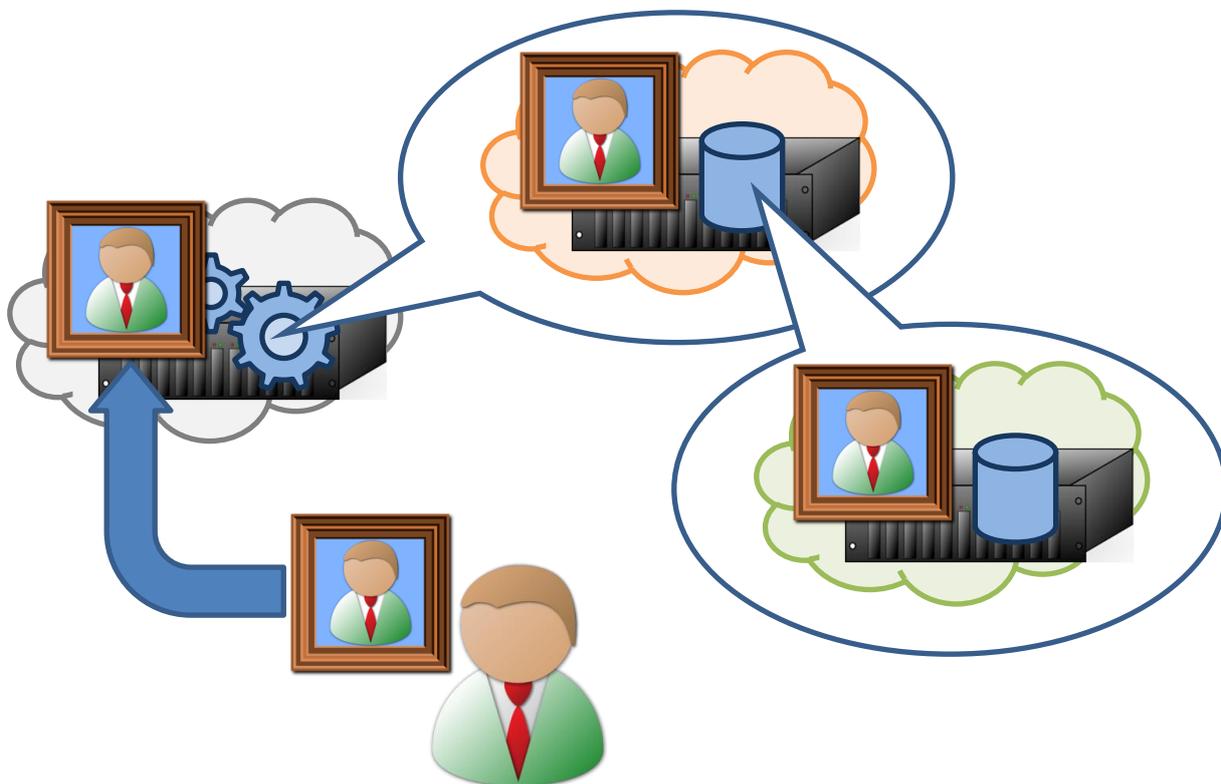


Figure 6: Intercloud example - Using multiple clouds to interact with each other for one process

All of these approaches share the same motivation: keeping cloud services up and running (*availability*) even if the hardware restrictions are exhausted. For the special case of Hybrid Clouds, an additional perceived advantage consists in the fact that – in contrast to using the public commodity cloud alone for all workloads – the provider of the public cloud does not learn much about the calculations of the cloud user, neither its processes nor its data (depending on the type of outsourcing). Only those processes and data that happen to be outsourced due to a peak in workload are getting disclosed to the provider of the public cloud, whereas all other details of the cloud services are hidden (*confidentiality*) within the private cloud. Obviously, the degree of security achieved by this restriction largely depends on the selection of workloads to outsource in event of a workload peak, so this aspect of the *Hybrid Cloud* approach is of high relevance for a risk assessment.

5.2.3.4 Homomorphic Encryption

Often labeled as the “holy grail of cryptology”, the approach of the so-called *fully homomorphic encryption scheme* consists in defining an encryption algorithm that allows for arbitrary modifications of the plaintext, performed by manipulating the ciphertext only, and without disclosing any information to the entity that actually performs the modifications to the ciphertext. For the particular case of cloud computing, a proper realization of that approach would enable a cloud provider to offer arbitrary data modification services (video rendering, file conversion, spreadsheet calculations etc.) while being able to guarantee (by means of a

cryptographically sound proof) that the cloud provider does not learn anything about the data it modifies itself.

Though some early research results surfaced (see Gentry¹⁶⁰), the use of this approach for real-world purposes is considered rather limited yet. This is due to its computational complexity and ciphertext storage requirements.

However, the use of any sort of homomorphic encryption schemes (not necessarily fully homomorphic ones) in the context of cloud computing holds a lot of promises. Assuming that the cloud user can encrypt some data, send it to the cloud provider, have it transformed in arbitrary ways – without the cloud provider learning anything about the contents of the ciphertext it modifies (*confidentiality*) – and getting the result back for decryption and usage is highly desirable for most types of cloud computing usage. If that approach could be implemented in a consistent, standardized, provably secure manner, the full potential of cloud computing would be unfolded.

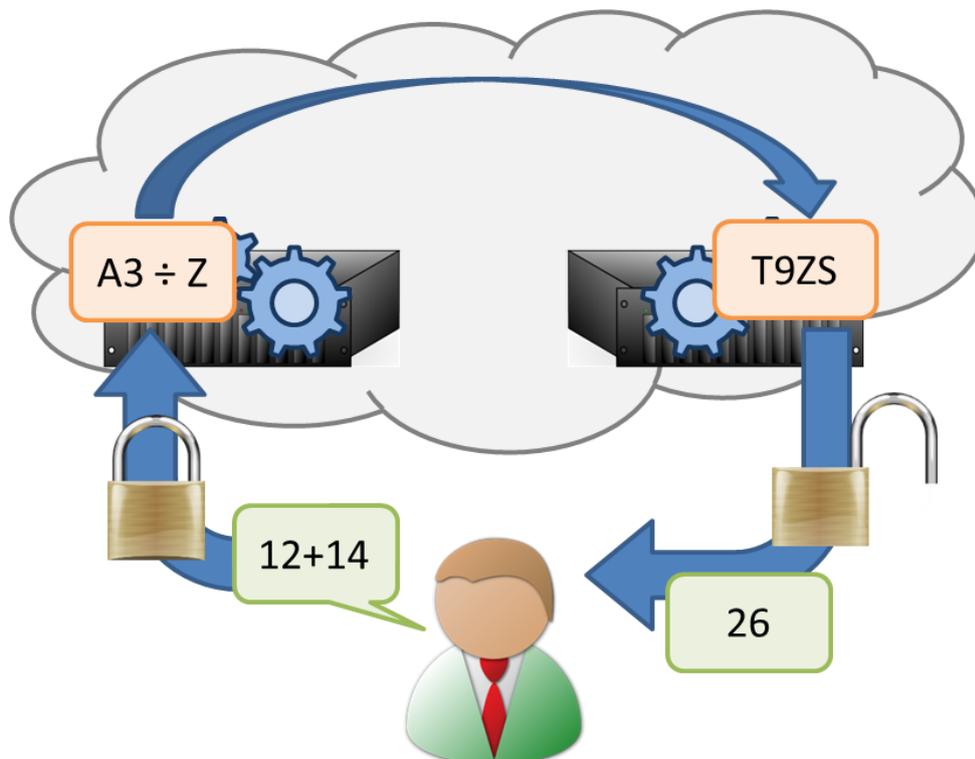


Figure 7: Homomorphic Encryption using one single cloud

Early results on real-world application schemes are e.g. given by *Jensen and Kerschbaum*¹⁶¹ for the specific domain of XML transformation in the cloud, or by *Sander, Young, and Yung*¹⁶² for basic string computations on encrypted strings.

¹⁶⁰ Craig Gentry: *A Fully Homomorphic Encryption Scheme*. Ph.D. Thesis, Stanford University, 2009;

Craig Gentry: *Fully homomorphic encryption using ideal lattices*. Proceedings of the 41st Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, pp. 169-178, 2009.

¹⁶¹ Meiko Jensen, Florian Kerschbaum: *Towards Privacy-Preserving XML Transformation*. IEEE International Conference on Web Services, Washington, DC, USA, pp. 65-72, 2011.

¹⁶² Tomas Sander, Adam L. Young, Moti Yung: *Non-Interactive CryptoComputing For NC¹*. 40th Annual Symposium on Foundations of Computer Science, New York, NY, U.S.A., pp. 554-567, 1999.

5.2.3.5 Secure Multi-Party Computation Clouds

Comparable to the approach of homomorphic encryption, the promise of secure computation is to perform a complex calculation in such a way that only the initiator gets the final result – in best cases along with a correctness argument (*integrity*) – whereas the other entities involved in the calculation, i.e. the cloud provider, do not learn anything about that result (*confidentiality*). However, in contrast to homomorphic encryption, the goal of secure computation is to compute a certain result jointly with a set of n parties, where each party takes responsibility for a certain fragment of the execution, and may also bring in some secret computational inputs of its own. If n is larger than two, one talks about secure multiparty computation.

As with the common cryptographic algorithms like encryption and digital signatures, secure multiparty computation protocols are designed in a way that allows for performing a mathematical proof of soundness. Thus, a provably secure multiparty computation allows for calculating its result in a way that none of its initial assumptions are violated.

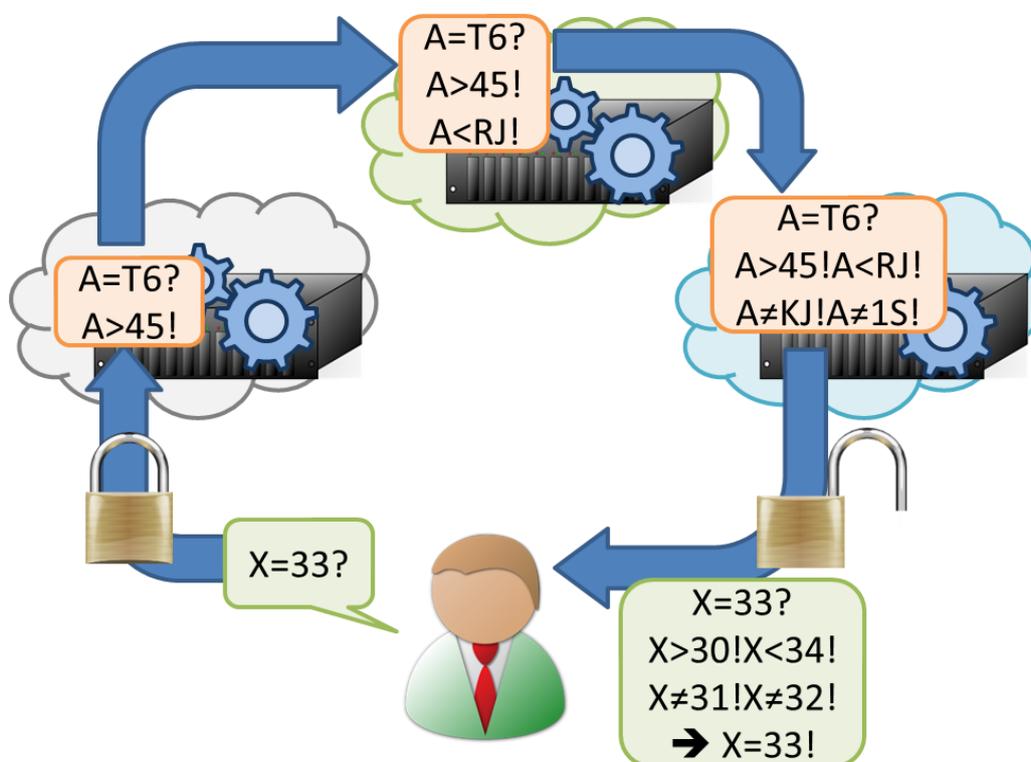


Figure 8: Secure Multi-Party Computation using multiple clouds

A common example of secure computation protocols is Yao's Millionaires' Protocol. In its original appearance, the setting involved two millionaires, which wanted to see who of them is richer— but without revealing their respective total amount of money to the other millionaire. Here, the restricting conditions are that a solution must guarantee that a) the result is true, and b) neither of the two millionaires learns anything about the amount of money of the other millionaire. Extending a solution of that problem to more than two millionaires results in a secure multi-party computation protocol. The theoretical deployment clearly offers privacy benefits with regard to computations on starting information that shall remain confidential. Although this approach might face limitations applied to more complex processes.

In the specific context of cloud computing, application of such secure computation protocols is a promising domain of research, however, existing secure computation protocols commonly have severe restrictions, e.g. in terms of performance. However, if applied to the

cloud computing scenario, common realizations use multiple cloud providers to implement the parties of the protocol, thereby exploiting the inherent assumption that these cloud providers do not collaborate maliciously against the cloud user. Either way, in the reduced setting of a two-party secure computation, common protocols are performed between the cloud user and a single cloud provider. Depending on the type of protocol, this allows for performing some more complex calculations on the cloud user's data without revealing too much information to the cloud provider (see e.g. *Jensen and Kerschbaum*¹⁶³).

5.3 Specific Enablers from the TClouds Architecture

The TClouds infrastructure fosters the use of the multi-cloud paradigm in several ways. Based on the previous works performed within the TClouds project scope, the following sections iterate over all of these approaches, analyzing their particular requirements, conditions, and benefits in terms of legal and economic aspects.

As a general conclusion, it is valid to state that all assumptions and conditions identified for the general multi-cloud approaches (as discussed in the previous chapter) still hold for the specific approaches discussed here. More precisely, since all of the technical approaches developed within the TClouds project so far can be categorized into one of the described multi-cloud scenarios, or a mixture thereof, the general legal assessments performed for these scenarios still hold in the specific conditions of the particular TClouds realizations. In this sense, the TClouds project covers technical components for a broad range of all these multi-cloud scenarios, a fact that impressively illustrates the scope of the TClouds project as advancing the state of the art in cloud security.

5.3.1 TPM Virtualization

5.3.1.1 Fundamentals of TPM

A crucial aspect of all use of cryptography in terms of IT systems lies in the secrecy of cryptographic keys (or similar types of cryptographic tokens). If the key for an encryption scheme is disclosed, the encryption scheme itself is compromised, rendering all encrypted contents as being disclosed as well. Similarly, if the cryptographic key for a digital signature scheme gets revealed to unauthorized entities, a valid cryptographic signature may be used in unintended ways, such as violating access control restrictions (if the signature is used for authentication purposes) or hiding malicious modifications to critical documents (if the signature is used for guaranteeing integrity).

Either way, in today's computer landscape, with each individual computing device being host to many concurrent programs, and being used for multiple types of tasks, keeping a cryptographic key a secret has become a highly challenging problem. Cryptographic keys have to be stored in their original appearance anywhere in the computer system's memory; otherwise they would not be available for performing any encryption, decryption, or digital signature tasks. However, this opens up a potential for key leakage: any other piece of software that is executed on the same computer system may potentially manage to read the key from memory and have it transmitted to a scope controlled by an adversary, e.g. via the network interface and the Internet.

¹⁶³ Meiko Jensen, Florian Kerschbaum: *Towards Privacy-Preserving XML Transformation*. IEEE International Conference on Web Services, Washington, DC, USA, pp. 65-72, 2011.

In order to overcome this memory leakage problem of cryptographic keys, the Trusted Computing Group¹⁶⁴ developed a set of specifications for realizing a specific, hardware-supported computer module that allows the use of cryptographic keys without the necessity to store these in the (system-wide accessible) computer main memory. This module, the Trusted Platform Module¹⁶⁵, consists of a dedicated chip with integrated memory, storage, and CPU, that resides within an arbitrary computer system, and offers access to the specific cryptographic keys within the module only via a set of dedicated access interfaces.

Based on this key ability to securely store cryptographic keys, the TCG adopted a set of functionalities that such a TPM can provide, such as

- **Sealing:** binding a specific piece of data to a hash value that is stored in the TPM. Later on, the same data can be verified for modification: if the hash value over the same piece of data has changed, the data itself must have been changed (since the hash value was stored securely and integrity-guaranteed within the TPM chip).
- **Binding/Wrapping:** this functionality enables a TPM chip to securely store arbitrary amounts of cryptographic keys (or other types of critical data) on external storage devices, such as hard disks, USB sticks, or even magnetic tapes. This is realized by encrypting all of these critical data items with a single cryptographic key that is unique for every single TPM chip, and cannot be extracted from that chip without breaking its hardware. The encrypted keys then can be stored to arbitrary external devices, and once the same key is required in any context, it can be read from that external source, decrypted within the TPM chip, and handed over to the requesting application.
- **Internal Storage:** despite the use of external storage devices, modern TPM chips also contain a limited amount of memory internal to the chip itself. Thus, this internal storage may also be used to store cryptographic tokens, which then are not even outsourced in any encrypted form – a property of high interest if the cryptographic algorithm used for implementation of the Binding/Wrapping functionality within the TPM may one day become compromised. Data stored within the TPM chip itself are assumed to be perfectly safe, unless an adversary gains unlimited access to the TPM chip's hardware directly. Therefore, the level of security provided by a TPM in this respect is considered way higher than any software-based key storage solution that utilizes main memory or external storage devices.
- **Remote Attestation:** One of the most interesting utilizations of the TPM module is its remote attestation capability: by using a secret, internal key that is unique to every single TPM chip being manufactured, a TPM module is able to sign arbitrary types of data in a way that can be verified by everybody, but cannot be forged by any entity (unless gaining access to the particular TPM hardware). Thus, it becomes possible for the TPM to “attest” some conditions (e.g. the hash value over a piece of software that is to be run on the CPU next, or the actual timestamp of the computer clock) in a cryptographically secure manner. This attestation token can the even be communicated to external sources, via the Internet, arbitrarily: as long as the attestation token is not modified, its signature will allow arbitrary entities that the digital signature once was applied by means of exactly that single TPM chip, and no other entity. This guarantee can then be used to build more complex guarantees, resulting in concepts like TPM-supported authentication (e.g. of servers in a TLS handshake) or

¹⁶⁴ The Trusted Computing Group (TCG), <https://www.trustedcomputinggroup.org/>

¹⁶⁵ Trusted Platform Module (TPM), TCG Specifications, http://www.trustedcomputinggroup.org/resources/tpm_main_specification

secured boot loaders (by attesting the hash value of a piece of software prior to loading that piece of software into the computer's CPU).

5.3.1.2 TPM and Clouds: the Multi-Tenancy Problem

Though the overall advantages of the TPM module approach are obvious, their use in real-world system architectures is somewhat limited. This is also due to the fact that the PC era raised a computing landscape with so highly complex configuration options that they cannot be unified properly for realizing a valid TPM architecture that is not broken by things like applying a patch to the operating system kernel. In fact, TPM approaches like secure boot loading require a hash value of every valid software configuration to be stored within the TPM, and on startup comparing each of them to the hash value calculated over the particular piece of software present at time of startup. However, the advent of the cloud computing paradigm has changed the game drastically for the TPM architecture. In IaaS cloud environments, a cryptographically strong guarantee that the cloud server's hypervisor was loaded in TPM-secured boot loading, and was not modified since, is a highly desirable property of every IaaS cloud offering. It allows building up a *chain of trust*: if the hypervisor was not modified since its boot loading, and if the hypervisor verifies the hash value over every virtual machine image prior to loading that image into its system, the virtual machine instance can be guaranteed to be free from malicious modifications at booting time in the cloud. Thus, within the virtual machine instance, a cloud user may hook on to that guarantee, and realize additional security architectures based on TPM module technology – with the security level being derived from the TPM-supported secure boot loading of the hypervisor. Hence, this type of TPM-based secure boot in cloud systems is of high interest in the cloud computing security research community.

Again, as with the PC problem, the pitfall of cloud-based TPM usage is complexity. If a single cloud server was to handle n instances of a single virtual machine image only, its secure boot loading would be realizable with a single TPM hardware chip within the cloud server itself only. However, with the existing approaches of multi-tenancy, each cloud server has to server multiple virtual machine instances concurrently, with a high level of dynamics in terms of virtual machine starting, stopping, copying, or migration to/from other servers. Thus, it becomes impossible to store all TPM data for all of these virtual machines concurrently within the same TPM module. Furthermore, most off-the-shelf TPM modules are designed for a dedicated host system, and do neither support virtualization nor multi-tenancy. Hence, if all TPM data of all virtual machines would be stored in the single one hardware TPM of a cloud server, there would be a high risk of unintended interference, which would also violate the security guarantees intended to achieve with using TPM in the first hand.

In order to overcome these issues of multi-tenancy with TPMs in virtualized cloud environments, the TClouds project investigated the potential for virtualizing the functionality of the TPM chip itself, realizing a “virtual TPM module” as a software component of the hypervisor system, which again is protected by the single hardware TPM chip. This approach is to be detailed next.

5.3.1.3 The TClouds Approach to TPM Virtualization

At its core, the TPM virtualization efforts performed in the TClouds project focused on providing the full TPM functionality to all of the virtual machine instances running on a single cloud server hardware system. By means of extending the hypervisor implementation, the functionality of the TPM chip was implemented directly into the virtualization kernel (details are depending on the type of virtualization being used in the hypervisor, i.e. whether it utilizes emulation, para-virtualization, or hardware-supported virtualization). This way, the TPM functionality can be used by all virtual machine instances, just as if the host machine contained a single, dedicated TPM module just for their execution. Thus, all common approaches of using TPM functionality for securing applications can be used in a virtualized cloud environment exactly like in dedicated server hardware.

Furthermore, since a virtualized TPM implementation is no longer a dedicated hardware chip but a software component, the challenge of securing that software component has to be solved. If the virtual TPM is implemented at the level of the hypervisor, this implies that a successful attack on the hypervisor would potentially result in compromise of the (virtual) TPM, even though being performed by means of software only. This somewhat violates the assumptions about the security of TPM solutions.

Hence, another effort of the TClouds infrastructure copes with this threat again. By utilizing the (hardware) TPM module built into each cloud server, the execution of the hypervisor implementation itself is protected by means of TPM-based secure boot loading. Hence, it can be guaranteed that the hypervisor was not modified maliciously during its boot loading, hence the implementation of the virtual TPM (or vTPM) within the hypervisor was not tampered with. Furthermore, again by utilizing the hardware TPM of the cloud server, remote attestations can be performed to validly show that a known und trusted version of the hypervisor was booted. Thus, a cloud user can gain such a remote attestation token at any time in order to verify that the hypervisor was not modified maliciously, implicitly also protecting the integrity of the vTPM, and thereby re-establishing the chain of trust from the hardware TPM to the application residing in the virtual machine instance that utilizes the services offered by the vTPM.

Thinking ahead, the TClouds project did not only focus on this aspect of securing the hypervisor, but generalized this approach by covering other types of virtualized computing devices as well. One of these efforts is focused on protecting virtual network devices (such as virtual switches, hubs etc.) that are commonly used within IaaS clouds:

Similar to virtualization of hardware servers, the idea is to virtualize all network equipment required for interaction among virtual servers as well. Thus, complete network environments, and even full data centres can be virtualized by means of cloud computing technology. However, as with virtualized servers, also virtual network devices have a demand for proper protection against attacks. Again, the fundamental technique for providing this required level of security is the use of TPM modules. Here, the scope of a TPM protection is no longer limited to a single virtual machine running in a single hardware server, but merely stretches over a set of virtual servers, switches, and cables; a so-called *trusted virtual domain (TVD)*.

In this field, the TClouds research efforts have come up with a set of approaches to realize TPM-based protection for various aspects of TVDs, as e.g. in *Bleikertz and Groß*¹⁶⁶; *Abbadi*¹⁶⁷; *Bleikertz, Groß, and Mödersheim*¹⁶⁸; or *Silvestro et al.*¹⁶⁹.

5.3.2 The TwinClouds Approach

The usage of TPM chips in cloud server hardware supports a broad range of possibilities for securing parts of a virtualized cloud infrastructure, however, the applicability and usability of

¹⁶⁶ Sören Bleikertz and Thomas Groß: *A Virtualization Assurance Language for Isolation and Deployment*. IEEE International Symposium on Policies for Distributed Systems and Networks, 2001.

¹⁶⁷ Imad M. Abbadi: *Clouds Trust Anchors*. 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

¹⁶⁸ Sören Bleikertz, Thomas Groß, and Sebastian Mödersheim: *Automated Verification of Virtualized Infrastructures*. ACM Cloud Computing Security Workshop, 2011.

¹⁶⁹ Jacopo Silvestro, Daniele Canavese, Emanuele Cesena, and Paolo Smiraglia: *A unified ontology for the Virtualization domain*. Proceedings of the 1st International Symposium on Secure Virtual Infrastructures, pp. 617-624, 2011.

these approaches largely depends on the collaboration and good-will of the cloud provider. For instance, most public cloud providers do not invest into TPM-equipped server hardware explicitly, but merely stick to high performance server racks, or even commodity hardware. In such cases TPM hardening of cloud security properties is not a viable approach.

Addressing this gap, the TClouds research efforts came up with the TwinClouds approach¹⁷⁰ for realizing TPM-free yet secured executions of code in a commodity cloud environment. The technical basis for the TwinClouds approach is a homomorphic encryption scheme¹⁷¹ known as *garbled circuits*. In principle, this cryptographic technique allows for executing a particular piece of code without getting to know the details of the execution, nor the results being calculated. Therefore, the piece of code in question has to be prepared in an initial step, breaking it down into its most basic operations (i.e. binary operations like XOR, AND etc.), and encoding each of these operations using a specific cryptographic algorithm. Then, these encoded instructions can be transferred to an arbitrary, untrusted entity, which can “execute” this encrypted piece of code, and transmit back the result (if existing, it is also encrypted). Then, that result must be decoded in a final step, and the overall execution is completed.

Adapting this general cryptographic technique to the cloud computing paradigm leads to the TwinClouds approach: a secure but resource-constrained “personal cloud” is used to prepare the encrypted versions of the code (it has to be encrypted once per execution, resulting in high computational loads) and upload these encrypted code instances to the commodity cloud. Then, once the execution is actually needed, the commodity cloud takes one of the existing pre-encrypted pieces of code, executes it, and returns the result to the personal cloud. There, it gets decrypted, and the execution is done.

The advantage of this approach is that commonly, the commodity cloud server is way faster and has way more computational resources than the personal cloud. Hence, using this mode, the net execution time at the moment the execution gets necessary is faster, and hence more economic. On the downside, the approach requires the personal cloud to continuously “recharge” the set of ready-to-run execution instances at the commodity cloud, hence is in (close to) permanent operation, and nevertheless faces the risk of “drain” of execution instances.

In total, the TwinClouds approach provides a very high level of security, since the cryptographic keys are never revealed to the cloud provider at all (in contrast to all TPM-based solutions that host the keys at the cloud data centres). Moreover, the computations being performed in the TwinClouds model are provably secure and correct. The approach has a pitfall in case of a malicious cloud provider that tampers with the execution of the garbled circuits, but this leads to integrity violations that can be detected at the side of the personal cloud rather easily.

¹⁷⁰ Sven Bugiel, Ahmad-Reza Sadeghi, Thomas Schneider, and Stefan Nürnberger: *Twin Clouds: Secure Cloud Computing with Low Latency*. 11. Communications and Multimedia Security Conference, Ghent, Belgium, pp. 32-44, 2011;

Sven Bugiel, Stefan Nürnberger, Ahmad-Reza Sadeghi, and Thomas Schneider: *The Hare and the Tortoise: Bringing together Fast and Trusted Clouds*. Workshop on Cryptography and Security in Clouds, Zurich, Switzerland, 2011.

¹⁷¹ Garbled Circuits are not a (fully) homomorphic encryption scheme, because one cannot execute operators/operations solely on the encrypted data, but needs the Garbled Tables as look-up.

5.3.3 The DepSky Approach

As discussed above, the use of TPMs and the TwinClouds approach provide high-level security guarantees, but both approaches have their drawbacks. TPM puts a lot of requirements to the server hardware provider by a cloud provider, and contains some technical pitfalls in application. The TwinClouds approach requires a secure environment (the personal cloud) a priori, hence cannot be applied to all scenarios. Moreover, the existing limitations in terms of performance renders many use cases of the TwinClouds approach moot in terms of economics; performing an execution in the (secure) personal cloud completely may be cheaper and more reliable than outsourcing it to a commodity cloud by means of the TwinClouds approach.

Hence, a third major area of research of the TClouds project focused on other techniques suitable for improving cloud security conditions, especially by exploiting the use of multiple cloud providers. In this line, the DepSky approach by Bessani et al.¹⁷² demonstrates how to exploit the existence of multiple cloud providers (taking an inherent assumption that these do not maliciously collaborate against the cloud user) to realize a highly resilient and fault-tolerant type of cloud data storage. By storing the same piece of data on all cloud providers concurrently, the total availability of that particular data is strengthened. Even more, by applying an algorithm that solves the so-called *Byzantine Agreement Problem*¹⁷³, the DepSky approach even allows for compensating one malicious cloud provider that (maliciously or by accident) tries to cause confusion among the cloud providers, e.g. by claiming the same file to hold different data when speaking to different parties. The DepSky approach utilizes a specific secure multi-party computation protocol that provably solves the Byzantine Agreement Protocol, thereby exposing all modifications a single cloud provider may try to induce into the scope of a certain file stored on the cloud.

However, the major drawback of applying such a Byzantine Agreement Protocol is its performance: on the one hand, the algorithm requires at least four different cloud providers to join the protocol, on the other hand, each retrieval of a file requires a communication protocol of several rounds of interaction between all pairs of cloud providers involved. Hence, the advantage of fault-tolerance in data storage— – and the inherent guarantee of integrity— – comes at the cost of high retrieval time and exponential communication overhead.

Nevertheless, the DepSky implementation has shown the approach to be feasible, realizing the TClouds architecture's guarantee of resilience and fault-tolerance while keeping acceptable performance overheads.

¹⁷² Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando André, and Paulo Sousa: *DepSky: Dependable and Secure Storage in a Cloud-of-Clouds*. 6th ACM SIGOPS/EuroSys European Systems Conference (EuroSys'11), Salzburg, Austria, pp.31-46, 2011.

¹⁷³ Leslie Lamport: *The Weak Byzantine Generals Problem*. Journal of the ACM, Volume 30, pp. 668-676, 1983.

Chapter 6

List of Abbreviations

Table 4: List of abbreviations

BCR	Binding Corporate Rules
BSI	Bundesamt für Sicherheit in der Informationstechnik – English: Federal Office for Information Security; often referred to as German Information Security Agency (Germany)
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNIL	Commission Nationale de l'Informatique et des Libertés
COBIT	Control Objectives for Information and Related Technology
CoC	Code of Conduct
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
DPA	Data Protection Agency (or Data Protection Authority)
EC	European Commission
ECP	European Cloud Partnership
EEA	European Economic Area
ENISA	European Network and Information Security Agency
ETNO	European Telecommunications Network Operator's Association
EU	European Union
EU SCC	European Union Standard Contractual Clauses
FedRAMP	Federal Risk and Authorisation Management Programme (USA)
FISMA	Federal Information Security Management Act (USA)
FIPS	Federal Information Processing Standards (USA)

IaaS	Infrastructure as a Service
ICO	Information Commissioner's Office (The UK DPA)
ICT	Information and Communication Technology
ISMP	Information Security Management Program
ISO	International Organisation for Standardisation
IT	Information Technology
ITIL	Information Technology Infrastructure Library
NIST	National Institute of Standards and Technology (USA)
PaaS	Platform as a Service
PBCR	Processor Binding Corporate Rules
PbD	Privacy by Design
RAM	Random Access Memory
SaaS	Software as a Service
SCC	Standard Contractual Clauses
SLA	Service Level Agreements
SMEs	Small and medium enterprises
TClouds	Trustworthy Clouds
UK	United Kingdom
VM	Virtual Machine

Chapter 7

Bibliography

7.1 Literature

Adhikari, Richard

EU Cloud Strategy Ruffles US Industry Group's Feathers, E-Commerce Times, September 27th 2012,
<http://www.ecommercetimes.com/story/76264.html>

Bernstein, David

Ludvigson, Erik;

Sankar, Krishnar;

Diamond, Steve;

Morrow, Monique

Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability, 2009 Fourth International Conference on Internet and Web Applications and Services, Venice, Italy, pp. 328-336, 2009

Bessani, Alysson;

Correia, Miguel;

Quaresma, Bruno;

André, Fernando;

Sousa, Paulo

DepSky: Dependable and Secure Storage in a Cloud-of-Clouds. 6th ACM SIGOPS/EuroSys European Systems Conference (EuroSys'11), Salzburg, Austria, pp.31-46, 2011

Bleikertz, Sören;

Groß, Thomas

A Virtualization Assurance Language for Isolation and Deployment, IEEE International Symposium on Policies for Distributed Systems and Networks, 2001

Bleikertz, Sören;

Groß, Thomas;

- Mödersheim, Sebastian *Automated Verification of Virtualized Infrastructures*. ACM Cloud Computing Security Workshop, 2011
- Bugiel, Sven;
Nürnberger, Stefan;
Schneider, Thomas;
Sadeghi, Ahmad *The Hare and the Tortoise: Bringing together Fast and Trusted Clouds*. Workshop on Cryptography and Security in Clouds, Zurich, Switzerland, 2011
- Twin Clouds: Secure Cloud Computing with Low Latency*. 11. Communications and Multimedia Security Conference, Ghent, Belgium, pp. 32-44, 2011
- Buyya, Rajkumar;
Ranjan, Rajiv;
Calheiros, Rodrigo *InterCloud: utility-oriented federation of cloud computing environments for scaling of application services*. In Proceedings of the 10th international conference on Algorithms and Architectures for Parallel Processing, Busan, Korea, pp. 13-31, 2010
- Cavoukian, Ann *Privacy by Design - The 7 Foundational Principles*, originally published: August 2009, revised January 2011, <http://www.privacybydesign.ca>
- Celesti, Antonio;
Tusa, Francesco;
Villan, Massimo;
Puliafita, Antonio *Security and Cloud Computing: InterCloud Identity Management Infrastructure*. Seventh International Workshop on Emerging Technologies for Next Generation GRID (ETNGRID), Larissa, Greece, pp. 263-265, 2010
- Cloud Security Alliance (CSA) *Cloud Controls Matrix (CCM) Version 1.2*, https://cloudsecurityalliance.org/research/ccm/#_version1_2

	<p><i>Consensus Assessments Initiative Questionnaire (CAIQ),</i> https://cloudsecurityalliance.org/research/cai/</p> <p><i>GRC Stack: Governance, Risk Management and Compliance,</i> https://cloudsecurityalliance.org/research/grc-stack/</p> <p><i>Open Certification Framework</i> https://cloudsecurityalliance.org/research/ocf/</p> <p><i>Security, Trust & Assurance Registry (CSA STAR)</i> https://cloudsecurityalliance.org/research/initiatives/star-registry/</p> <p><i>STAR Registry Entries,</i> https://cloudsecurityalliance.org/research/initiatives/star-registry/</p>
EuroCloud Deutschland_eco e.V	<p><i>Leitfaden Cloud Computing Recht, Datenschutz & Compliance,</i> http://www.saas-audit.de/426/anforderungen/</p> <p><i>EuroCloud Star Audit</i> http://www.saas-audit.de/</p>
European Telecommunications Network Operator's Association (ETNO)	<p><i>Position Paper: Reflection Document on the EU Public Consultation on the Communication on a comprehensive approach on personal data protection in the European Union, published in January 2011</i></p> <p><i>Position Paper: Reflection Document replying to the public consultation on Cloud Computing, published in August 2011</i></p>
Gentry, Craig	<p><i>A Fully Homomorphic Encryption Scheme, Ph.D. Thesis, Stanford University, 2009</i></p>

Fully homomorphic encryption using ideal lattices, Proceedings of the 41st Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, pp. 169-178, 2009

Harnik, Danny;

Pinkas, Benny;

Shulman-Peleg, Alexandra

Side Channels in Cloud Services: Deduplication in Cloud Storage, IEEE Security & Privacy, vol. 8, no. 6, pp. 40-47, Nov.-Dec. 2010, doi:10.1109/MSP.2010.187

Hustinx, Peter

Data Protection and Cloud Computing under EU law, speech at the Third European Cyber Security Awareness Day BSA, European Parliament on 13 April 2010 in Panel IV: Privacy and Cloud Computing:

http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf

Jensen, Meiko;

Kerschbaum, Florian

Towards Privacy-Preserving XML Transformation. IEEE International Conference on Web Services, Washington, DC, USA, pp. 65-72, 2011

Jensen, Meiko;

Schwenk, Jörg;

Bohli, Jens-Matthias;

Gruschka, Nils;

Lacono, Luigi Lo

Security Prospects through Cloud Computing by Adopting Multiple Clouds, Fourth IEEE International Conference on Cloud Computing, Washington, D.C., U.S.A, pp. 565-572, 2011.

Juels, A.;

Kaliski Jr., B. S.

PORs: Proofs of retrievability for large files, Proceedings of the 14th ACM conference on Computer and communications security, 2007

- Kelly, Kevin *A Cloudbook for the Cloud*, 2007, http://www.kk.org/thetechnium/archives/2007/11/a_cloudbook_for.php
- Kroes, Neelie *Setting up the European Cloud Partnership*, speech at the World Economic Forum Davos, Switzerland, 26th January
http://europa.eu/rapid/press-release_SPEECH-12-38_en.htm?locale=en
- Lamport, Leslie *The Weak Byzantine Generals Problem*. Journal of the ACM, Volume 30, pp. 668-676, 1983
- Leach, Emily: *Data Protection Authorities Crack Down on Breach Offenders*, published 09.08.2011 on the website of the International Association of Privacy Professionals,
https://www.privacyassociation.org/publications/data_protection_authorities_crack_down_on_breach_offenders .
- Millard, Christopher *Proposed EU Data Protection laws unlikely to promote cloud computing*, Queen Mary University of London, 1 February 2012
<http://www.qmul.ac.uk/media/news/items/hss/63123.html>
- NIST *NIST Definition of Cloud Computing*, <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- Pfitzmann, Andreas;
Hansen, Marit *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, 2010
http://dud.inf.tu-dresden.de/Anon_Terminology.shtml
- Sander, Tomas;
Young, Adam L.;
Yung, Moti *Non-Interactive CryptoComputing For NC1*. 40th Annual Symposium on Foundations of Computer Science, New York, NY, U.S.A., pp. 554-567, 1999

Silvestro, Jacopo;

Canavese, Daniele;

Cesena, Emanuele;

Smiriglia, Paolo

A unified ontology for the Virtualization domain
Proceedings of the 1st International Symposium
on Secure Virtual Infrastructures, pp. 617-624,
2011

Trusted Computing Group (TCG)

*Trusted Platform Module (TPM), TCG
Specifications,*
http://www.trustedcomputinggroup.org/resources/tpm_main_specification

Weiss, Andreas

*Cloud Computing und SaaS - Transparenz und
Sicherheit durch das EuroCloud SaaS
Gütesiegel, 2. EuroCloud Workshop SaaS
Gütesiegel, Feb. 2010,*
http://www.eurocloud.de/files/2010/04/100428_Weiss_EuroCloud.pdf

7.2 Legislation

Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as: EU Data Protection Directive 95/46/EC)

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC (hereinafter referred to as: E-Privacy Directive) concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 (final), January 25th 2012

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

7.3 Official statements & opinions on EU and national level

7.3.1 European Commission

European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*, Communication COM (2010) 609 final of 4 November 2010

http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

European Commission - *Unleashing the Potential of Cloud Computing in Europe*

http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

Response to the Call for Evidence on the Current Data Protection Legislative, Framework carried out by the Ministry of Justice UK; Call for Evidence on the Current Data Protection Legislative Framework

<http://www.justice.gov.uk/consultations/docs/dpa-call-evidence-response-paper-28-01-11a.pdf>

7.3.2 Other EU bodies

ENISA – Cloud Computing: Benefits, Risks and Recommendations for Information Security,

<https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment>

ENISA – Cloud Computing Information Assurance Framework, 2009

<http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework>

ENISA – *Cloud Computing Risk Assessment*, 20 November, 2009

<http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment>

ENISA – Procure Secure: A guide to monitoring of security service levels in cloud contracts, 2 April 2012

<http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts>

ENISA – Security and Resilience in Governmental Clouds, 2011

<http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector>

7.3.3 Article 29 Data Protection Working Party

Article 29 Data Protection Working Party, **WP 74**, *Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, adopted on 3rd June 2003

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf

Article 29 Data Protection Working Party, **WP 168**, *The Future of Privacy – Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, adopted on 01 December 2009

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Article 29 Data Protection Working Party, **WP 172**, *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive*, Adopted on 13 July 2010

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf

Article 29 Data Protection Working Party, **WP 173**, *Opinion 3/2010 on the principle of accountability*, adopted on 13 July 2010

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

Article 29 Data Protection Working Party, **WP 187**, *Opinion 15/2011 on the definition of consent*, adopted on 13 July 2011

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Article 29 Working Party, **WP 195**, Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, adopted on 6 June 2012

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

Article 29 Data Protection Working Party, **WP 196**, *Opinion 05/2012 on Cloud Computing* adopted on 01 July 2012

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

7.3.4 National Level

Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, *Orientierungshilfe – Cloud Computing*, Version 1.0, adopted on 26 September 2011

http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

BSI – 100-2 *IT Grundschutz Methodology*, Version 2.0, 2008,

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile

BSI – 100-3 *Risk analysis based on IT Grundschutz*, V 2.5, 2008,

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile

BSI – *White Paper “Security Recommendations for Cloud Computing Providers*, no date,

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile

Centre for Information Policy Leadership as Secretariat to the Galway Project, *Data Protection Accountability: The Essential Elements*, A Document for Discussion, October 2009

CNIL - *Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing*,

http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

ICO's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998,

http://www.ico.gov.uk/~/_media/documents/library/Corporate/Research_and_reports/guidance_issue_of_monetary_penalties_draft_for_consultation.pdf

ICO – *Deleting Personal Data*, Version 1.0, 16 August 2012

http://www.ico.gov.uk/for_organisations/guidance_index/~/_media/documents/library/Data_Protection/Practical_application/deleting_personal_data.ashx

International Conference of Data Protection and Privacy Commissioners, *Madrid Resolution*, held in Madrid on 5 November 2009

http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/InternationalDS/2009MadridResolution.pdf?__blob=publicationFile

International Conference of Data Protection and Privacy Commissioners, , *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data*, held in Madrid on 5 November 2009

http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/InternationalDS/2009MadridResolution.pdf?__blob=publicationFile

The National IT and Telecom Agency Copenhagen, Denmark: *New Digital Security Models - Discussion Paper*, February 2011

U.S. Federal Information Security Management Act of 2002

<http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

U.S. Federal Risk and Authorization Management Program

<http://www.gsa.gov/portal/category/102371>

US Health Insurance Portability and Accountability Act of 1996

<http://www.gpo.gov/fdsys/search/pagedetails.action?granuleId=CRPT-104hrpt736&packageId=CRPT-104hrpt736>

US Payment Card Industry Data Security Standard

https://www.pcisecuritystandards.org/security_standards/index.php