SEcure Cloud computing for CRitical Infrastructure IT

Contract No 312758

Deliverable D.2.7
Summary of legal aspects

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris

Document control information

Title	Summary of Legal Aspects	
Creator	KIT-legal	
Editor	Silvia Balaban	
Description	This deliverable contains all legal consideration from the project	
Classification	☐ **Red** – Highly sensible Information, limited access for: ☐ **Yellow** – restricted limited access for: ☐ **Green** – restricted to consortium members ☒ White – public	
Reviewers	☐ AIT ☒ ETRA ☐ IESE ☒ KIT ☐ NEC	☐ ULANC ☐ MIRASYS ☐ OTE ☐ VLC ☐ AMARIS
Review status	☐ Draft ☐ WP Manager accepted ☒ Co-ordinator accepted	
Action requested	☐ to be revised by Partners involved in the preparation of the Project Deliverable ☐ to be reviewed by applicable SECCRIT Partners ☐ for approval of the WP Manager ☐ for approval of the Project Co-ordinator	
Requested deadline	31/12/2015	

Versions

Version	**Date**	**Change**	**Comment/Editor**
1	30.11.2015	First complete draft	Silvia Balaban
2	15.12.2015	Full document review	Santiago Caceres
3	18.12.2015	Full document review	Roland Bless

Abstract

The basic characteristic of cloud computing is its “black box” nature in the meaning that it is not visible what actually happens within cloud-based systems. A main reason for this intended opacity is the fact, that the user of cloud-based services should not be confronted with the technical details of the system, as the use of the system does not require an understanding of the functioning of cloud based services. However, from a legal perspective especially in the fields of evidence and data protection law a more transparent behaviour is necessary. As evidence law deals with questions about which party has to prove which facts, the respective cloud computing parties need to be equally aware of what happens in the cloud with the outsourced data. If the proofs however are in the area of the cloud provider it is extremely difficult for the cloud user to really assess whether these proofs stemming from the realm of the provider are truthful or have just been tampered by the provider in order to win the lawsuit. Therefore within the SECCRIT project we are considering how to enable the cloud user a direct access to potential proofs which does not need an assistance of the provider. Within the field of data protection law, transparency is as well needed especially in order to fulfil the rights of the data subject. It is therefore a core challenge how the technical properties of the cloud comply with the legal requirements and thus to design technical solutions which can help to realize them. Technologies developed within the SECCRIT project were therefore evaluated according to the fulfilment of the legal requirements. In this deliverable we bring together all legal considerations from the project. This includes the legal evaluation of evidence and data protection law in the context of cloud computing. We not only assess the use cases from a legal perspective, but we also provide a techno-legal assessment of the developed technologies. Furthermore we provide adaptations of the legal framework as well as possibilities on how to integrate SECCRIT technologies. This document also outlines how the technical outputs have been influenced by the legal work. Therefore, all techno-legal issues are addressed and best practice recommendations for the use of cloud computing in the critical infrastructure domain are given. This work builds on deliverables D2.2 on legal fundamentals, D2.3 Analysis of security-related aspects, D2.4 National Data Protection Consultation Results, and the following publications:

- S. Balaban and F. Pallas: „Haftung und Beweis bei geschachtelt komponierten Cloud-Services“, InTeR 2013, 193-198
- S. Balaban and F. Pallas: “Non simplificate nubes! Ein rechtlicher Blick hinter die Kulissen informatischer Cloud-Forschung”, in 14. Herbstakademie, 2013

Table of Contents

Table of Figures

1 Introduction

Cloud computing raises numerous legal questions. The outsourcing of sensitive data into the cloud can lead to significant challenges and must be treated very cautiously especially in the domain of critical infrastructures. Generally speaking, cloud computing already unifies legally known concepts like application service providing (ASP), IT-outsourcing, webhosting etc. However it goes far beyond these services as its major characteristic consists in assembling different units to another new composed one. A core challenge is in this context that far more than two parties interact, making it more difficult to really assess what actually happens within cloud based systems and who is actually responsible for what.

Fulfilling the legal requirements from the very beginning of a project is essential, as the developed technologies need to be legally compliant in order to permit their use in practice. This so called “privacy by design” approach has been followed in the SECCRIT project from the very beginning. The scope of the SECCRIT project is therefore the development of legally conforming technologies, which aim to strengthen the legal position of the cloud user and thus the data subject by making the cloud “transparent”. The purpose of this document is therefore to show why a more transparent cloud is needed and how this has been technically realized.

This document therefore summarizes the legal considerations from the perspective of evidence and data protection law that need to be taken into account, when using cloud computing, as especially in these fields legal deliberations have not been or at least not sufficiently been addressed.[1]

In a first section requirements in the field of critical infrastructures will be outlined. Afterwards an in-depth analysis of evidence and data protection issues will be provided, which will also take the Finnish and Spanish regulations into account in order to show national legal compliance with the demo case countries. All these deliberations will be explained along the SECCRIT use case scenarios. In the further course of the deliverable recommendations will be provided. A legal assessment of the developed technologies within the SECCRIT project concludes this deliverable, followed by (legal) possibilities to integrate the developed technologies in the legal framework.

1.1 Definition of used terms within this deliverable

As we agreed within the SECCRIT project on the following architectural framework (Figure 1) we will therefore describe the different roles and map them to the roles “cloud user” and “cloud provider”, which will be used in the further course of the deliverable.

We understand the CI Service User as the cloud user and thus his contractual partner the CI Service Provider as “the cloud provider”. Thus, whenever we use the term “cloud user” we refer to the CI service user on the top level of the architectural framework. As a consequence we understand the CI Service provider as the “cloud provider”. The tenant infrastructure provider and the cloud infrastructure provider are therefore subcontractors of the “cloud provider” thus of the CI Service Provider.

In order to keep the reading of this deliverable in a simplified manner we restrict the use of the words to “cloud user”, “cloud provider” and “subcontractors”.

[1] The legal findings are only for research purpose and therefore only valid for this project. They do not aim at providing legal advises for other cases.

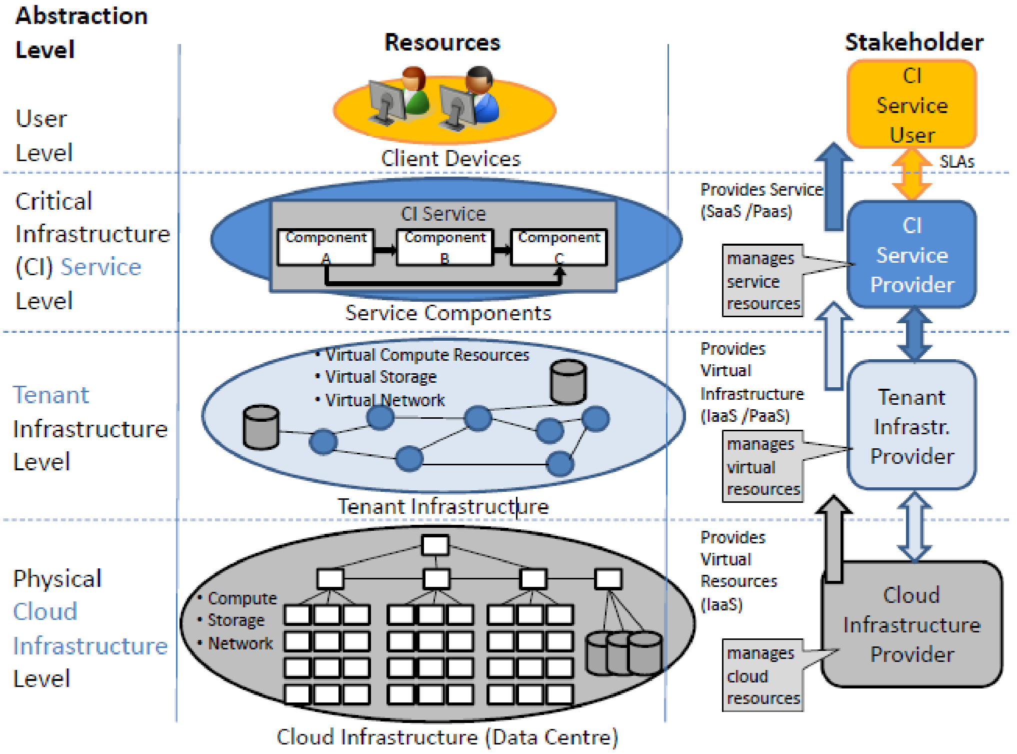
Abstraction Level
Resources
Stakeholder
User Level
Client Devices
CI Service User
SLAs
Critical Infrastructure (CI) Service Level
CI Service
Component A
Component B
Component C
Service Components
Provides Service (SaaS /Paas)
manages service resources
CI Service Provider
Tenant Infrastructure Level
• Virtual Compute Resources
• Virtual Storage
• Virtual Network
Tenant Infrastructure
Provides Virtual Infrastructure (IaaS /PaaS)
manages virtual resources
Tenant Infrastr. Provider
Physical Cloud Infrastructure Level
• Compute
• Storage
• Network
Cloud Infrastructure (Data Centre)
Provides Virtual Resources (IaaS)
manages cloud resources
Cloud Infrastructure Provider

FIGURE 1: ARCHITECTURAL FRAMEWORK

1.2 Use Cases

As within the SECCRIT project two use cases have been established the legal problems shall be depicted along the use case scenarios in order to illustrate in a more understandable way the occurring problems. We separate the evaluation of these two cases and explain the liability and evidence law problems along the first case and the data protection law problems along the second one.

1.2.1 Storage and processing of sensitive video surveillance data (Mirasys Use Case)

A large subway station in a European metropolis suffers from vandalism and lack of security. This causes the subway operator (MetroSub Inc.) huge costs and disturbs the traffic heavily. To improve the security at the station, the operator contracts City Sec Ltd, a security service provider. According to the contract, the security company installs 100 surveillance cameras in the station. If something suspicious can be noticed by the cameras, the alarm centre operator sends a patrol of guards to the site – this reduces costs as the number of guards on duty can be kept on a minimum level. To reduce the operator costs, CitySec decides to take advantage of the latest Video Analytics technology, which is supposedly capable of detecting loitering, gathering or suspicious behaviour of people in areas where they should not be. This leads to a situation, where for most of the time, there is no human operator but the system relies on the automatic alarming system. Some of the retailers and café owners at the station have already installed cameras in their premises. The security company will have access to these cameras too. As the company is also planning to take over the guarding of other subway stations, they decide to take the whole service to the cloud. The cloud application is delivered by a specialist IT company called TenSYs Ltd., who further places an order with a CloudCorp Ltd., a supplier of servers for data storage and processing. Additionally, they contract TelCom Ltd., a telecom operator to take care of data communications. The system is set up, and everything goes well for a while before two unpleasant and messy incidents occur.

1.2.1.1 *Act of vandalism in the night*

One night the station is demolished again during closing hours. The direct damages exceed 100.000 € and the station is closed for a day. The mess is discovered first in the morning when the station is opened. The security guards have not intervened as they have not received an alarm. No image recordings from the night can be found. No logs can be found that could tell the reason for the problem. This means that either the cameras have not sent the images to the cloud, the analytics system has not received the images, the analytics system has failed to detect the anomalies, the alarming system has not been able to transmit the alarms to the guards, an unintentional shutdown of the system or any part of it, an intentional interference with the system from inside, a hacker-type attack against the system, or a combination of the above occurred. MetroSub claims for indemnification from the operators. Nobody knows what actually caused the trouble – CitySec, TelCom, TenSys and CloudCorp blame each other. MetroSub sues CitySec.

1.2.1.2 *The misbehaving politician*

Another night, a known politician travels through the station after an evening party. Having had a few glasses too much, he needs to vomit in a trash can. No one sees this except one of the cameras. Next morning, the picture of the vomiting politician is in a tabloid newspaper. Nobody knows how it has come to the editors, who refuse to reveal the source. No logs are available anywhere in the system showing that the images had been copied or exported from the system.

1.2.2 Hosting critical urban mobility services in the cloud (Valencia Use Case)

As the Valencia use cases (Story 1 Moving to the cloud and Story 2 Evaluating risks with data in the cloud) are more designed as a case in which managers decide to move part of the infrastructure in the cloud and want to know what they need to respect, this case will not be used as an example for showing the upcoming legal problems, due to the fact that this deliverable will provide the legal challenges and therefore the solution of this use case.

2 Critical Infrastructures and Cloud Computing

Throughout the last years the European Union took several approaches towards addressing the protection of critical infrastructures on a European level. After adopting a Green Paper[2] on a European Programme for Critical Infrastructure Protection (EPCIP) in 2005, the European Commission set out the principles, processes and instruments proposed to implement EPCIP in a 2006 communication[3].

[2] European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final.

[3] European Commission, Communication on a European Programme for Critical Infrastructure Protection, COM(2006) 768 final.

One of these implementation measures, the directive 2008/114/EC on the identification and designation of European critical infrastructures[4], defines "critical infrastructures" in its article 2(a) as follows: "*'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;*" Another definition within this directive copes with infrastructures at a European level: "*'European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure*", Art. 2(b) of the directive.

2.1 Critical Information Infrastructures (CII)

In today's information society, more and more critical infrastructures or parts thereof consist of or rely on network and information systems. The electrical power grid, for example, consisted few decades ago mostly of electrical or mechanical parts without much intelligence or interconnection between different operators and their assets. Future power grids will not only have intelligent control technologies at higher levels like power plants and network operators, intelligent and interconnected control devices will most probably be integrated into most households[5] and even household appliances. The power grid infrastructure is a good example for cross-border, cross-sector and even cyclic dependencies between different critical (information) infrastructures. The power grid is interconnected all over Europe and production and distribution of electrical power does not stop at member state borders. Management of the power grid depends more and more on information infrastructure which, in turn, depends on electrical supply in order to function correctly. Many other sectors of critical infrastructure operation depend already today heavily on information systems and network structures, like for example the banking sector, stock exchanges and supply chains for everyday needs of the population like food. It can be stated, that interdependencies between physical and electronic infrastructures increase and that boundaries between protection of critical infrastructure and critical information infrastructure are therefore becoming more and more blurred.[6]
The planned European measures with regard to the protection of critical infrastructures acknowledge and stress the fact, that today's information society and the infrastructure necessary to maintain vital societal functions depends on the functioning of underlying ICT-infrastructures.[7] Specific definitions for ICT-related critical infrastructures and their protection can be already found in the 2005 Green Paper of the European Commission. The Commission herein defines "*Critical Information Infrastructure (CII)*" as "*ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).*" [8] The same paper also contains a specification of what "*Critical Information Infrastructure Protection (CIIP)*" means: "*The programs and activities of*

[4] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
[5] European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final.
[6] Centre for European Policy Studies (CEPS), Protecting Critical Infrastructure in the EU, 2010 gives a good overview over interdependencies between different critical infrastructures.
[7] Centre for European Policy Studies (CEPS), Protecting Critical Infrastructure in the EU, 2010.
[8] European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, p. 19.

Infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimizing the recovery time and damage. CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective."[9] The Green Paper also acknowledges that ICT-enabled infrastructures need particular attention with regard to existing cross-sector and cross-border interdependencies.[10]

2.2 The Proposal for a NIS-Directive

A very important part of the efforts to improve cyber security and the protection of critical infrastructures within the EU is the 2013 proposal of the European Commission for a European directive aimed at achieving a high common level of network and information security across the European Union[11] (NIS-directive). A European directive normally addresses only the member states directly and requires them to undertake certain actions to achieve the intended outcomes, whereas citizens and companies residing within the member states are not directly bound by the directive but only by the national legislation and other national measures undertaken in order to implement the directive.

The planned NIS directive has two main objectives. On the one hand, network and information security shall be fostered by obliging member states to adopt national measures improving network and information security, on the other hand, reporting, communication and cooperation regarding NIS incidents should be enhanced on a national and on an EU-wide level alike.

The planned directive will have a broad scope of application, since the term "network and information system" as defined in article 3(1) of the directive comprises "*an electronic communications network within the meaning of Directive 2002/21/EC, and*" "*any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as*" "*computer data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.*" This very broad definition shows that nearly every physical asset and even data related to network and information systems is intended to be comprised. The range of application is, however, narrowed down by focusing it on assets belonging to infrastructures vital for society as explained below.

The directive also defines what "*security*" within the context of the directive means: "*'security' means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system;*"

Article 3(8) of the proposal defines the term "*market operator*". According to this provision, "market operator" within the meaning of the directive is any "*operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy,*

[9] European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, p. 19.
[10] European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, p. 19.
[11] European Commission, COM(2013) 48 final, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. (NIS-Directive)

transport, banking, stock exchanges and health, […]", Art. (3(8) b)), but also any "*provider of information society services which enable the provision of other information society services, a non-exhaustive list of which is set out in Annex II;*", Art. (3(8) a)).

"Cloud service providers" are even mentioned explicitly within the NIS directive as possible addresses of the planned measures: The referred list in Annex II of the directive mentions amongst others "*cloud service providers*" as market operators within the meaning of Art. (3(8) a)) of the directive.

The definitions in the NIS directive and the definitions of the European Commission concerning critical information infrastructures implicate that there is a distinction between information infrastructures that are critical infrastructures themselves and information infrastructures that are essential for the operation of other critical infrastructures[12]. The ENISA[13] maps this distinction to cloud computing services used in critical infrastructures and points out that a clear distinction between "cloud computing services that are critical themselves" and "cloud computing services that are critical for other critical services" is not always possible and hence refrains (at least to some part) from such distinction and calls the cloud computing services in both cases "critical"[14].

The point made by the ENISA when stating that a distinction between cloud services that are critical themselves and cloud services that are critical for other critical services seems, however, valid. One the one hand, a clear distinction is not always possible and would probably depend on to what extent a critical (information) infrastructure service consists of cloud assisted services. On the other hand, it seems reasonable to treat both cases as equally critical, since in most scenarios it will probably not make much difference whether a critical cloud service itself fails or whether another critical service fails because essential underlying cloud infrastructures fail.

Critical infrastructure providers and cloud service providers falling within the scope of the planned NIS-directive will be affected in various ways with regard to security measures and incident reporting obligations.

Art. 14 of the proposed NIS directive will require member states to "[…] *ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations*." The provision provides further detail by stating that: "*Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimize the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.*"

The planned NIS directive also aims at establishing more governmental control over network and information security with regard to those market operators within the scope of the planned directive. Art. 15 will require member states to equip the competent authorities with the necessary power to investigate cases of non-compliance with requirements set by the NIS Directive. Furthermore, member states must equip these authorities with the power to require entities falling within the scope of the directive to "*provide information needed to assess the security of their networks and information systems, including documented security policies;*" and to *"undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority."*

[12] For this distinction made by the European Commission see ENISA, Critical Cloud Computing, Version 1,0, December 2012, Section 3.2.

[13] European Union Agency for Network and Information Security (ENISA).

[14] ENISA, Critical Cloud Computing, Version 1,0, December 2012, Section 3.2.

These planned provisions indicate, that assessment and documentation of risks and security measures related to network and information systems and corresponding responsibilities of market operators and public administrations using such systems will become even more relevant under future legislation. Recital 26 of the planned directive, mentions that "*The public administrations and market operators should ensure security of the networks and systems which are under their control. These would be primarily private networks and systems managed either by their internal IT staff or the security of which has been outsourced. The security and notification obligations should apply to the relevant market operators and public administrations regardless of whether they perform the maintenance of their network and information systems internally or outsource it*."

Furthermore, the planned directive foresees obligations for public administrations and market operators to notify to the competent authorities in case of incidents having a significant impact on the core services they provide (Art. 14(2) of the proposed NIS directive). Recital 29 of the proposal mentions, that the competent authorities should be able to obtain "[…] *reliable and comprehensive data about actual incidents that have had an impact on the operation of network and information systems*." This indicates, that technical and organizational possibilities to trace and investigate security incidents and their causes in the aftermath will also gain substantially in relevance under the planned NIS directive.

The concrete legal obligations arising for operators of network and information systems will depend on what the final version of the directive requires and how these requirements are transferred into national legislation of each member states.

2.3 Reports of ENISA related to Cloud Computing in Critical Infrastructures

The European Network and Information Security Agency (ENISA) already published several reports on cloud computing, some of which deal especially with governmental use of cloud computing and even with the use of cloud computing in critical infrastructures.

In 2012 the ENISA published a report titled "Critical Cloud Computing". In this report, the ENISA calls cloud computing as seen from a critical infrastructure perspective a "*double edged sword*", explaining that on the one hand, cloud computing may improve security and resilience, while on the other hand outages or security breaches may have far worse consequences.[15]

The ENISA gives four exemplary scenarios were cloud computing deployments are used in critical infrastructures and different types of possible threats are analysed with regard to these scenarios. The ENISA then draws the following conclusions:[16]

- Cloud computing is critical itself and other critical sectors depend on cloud computing
- Due to redundancy, cloud computing can strengthen resilience of systems against local incidents like power failures or natural disasters
- Due to its elasticity, cloud computing can mitigate the risks of overloads or DDoS attacks
- Concentration of resources in cloud computing can multiply impacts of cyber attacks
- Infrastructure as a Service and Platform as a Service are most critical

[15] ENISA, Critical Cloud Computing, Version 1,0, December 2012.
[16] ENISA, Critical Cloud Computing, Version 1,0., Section 5.

Measures recommended by the ENISA for cloud computing in critical infrastructures include risk assessment with special regard to cloud computing in critical infrastructures, appropriate security measures and improved incident reporting.[17]

With regard to risk assessment, the ENISA recommends, that cloud computing services and large data centres should be included in national risk assessments concerning critical infrastructure. Not only should dependencies of critical infrastructures on cloud computing services as such be taken into account, but furthermore logical and physical dependencies should be made transparent in risk assessments for critical infrastructures in order to clarify which critical infrastructures depend on which cloud computing services.[18]

With regard to security measures, the ENISA recommends, besides the obvious fact that security measures must be implemented in the best possible way, to foster exchange of best practices concerning security. Furthermore, it is pointed out that there should not only be physical redundancies but also logical redundancies like for example different defence layers.[19] Furthermore, the ENISA points out the importance of audits, tests and exercises and puts a special focus on the fact, that with regard to the complexity of cloud infrastructures and rapid changes in ICT systems and software periodic (e.g., yearly) audits are devalued to some part, since they are not capable of reflecting these continuous changes.

In 2013 the ENISA published a report titled “Cloud Security Incident Reporting” aimed at increasing awareness of the importance of security incidents reporting in cloud environments for private and public bodies involved in critical infrastructure operation.[20] In order to better incident reporting schemes, the ENISA proposes an approach under the motto “*Think big, but start small*”, meaning that an approach starting with the most critical cloud computing services and the easier to detect incidents followed by iterative refinement will be most promising.[21]

This report points out the importance of incident reporting clauses in cloud computing contracts concluded by operators of critical infrastructures with regard to existing and future legal obligations for incident reporting critical infrastructure operators themselves are or will be subject to. Such obligations can only be duly fulfilled by operators of critical infrastructures if they are fully aware of security measures in place and security incidents happening within outsourced cloud environments they use in their business operations. In order to achieve this, the ENISA recommends addressing of incident reporting obligations in contracts and SLAs concerning the participation of cloud computing providers in critical infrastructures. Similar advice is given to governmental authorities who should, according to the ENISA, address incident reporting in their security requirements.[22] This underlines, that any use of cloud computing in critical infrastructures will require measures to overcome the opaqueness inherent to complex cloud computing environments.

The report encourages collaborative approaches including industry, businesses and customers as well as national and European authorities, pointing out that voluntary collaboration with regard

[17] ENISA, Critical Cloud Computing, section 5.
[18] ENISA, Critical Cloud Computing, section 5.1.1.
[19] ENISA, Critical Cloud Computing, section 5.1.2.
[20] ENISA, Cloud Security Incident Reporting, 2013.
[21] ENISA, Cloud Incident Reporting, p. 29f.
[22] ENISA, Critical Cloud Computing, Section 5.1.2.

to security and NIS-incidents could be a promising starting point on the way to improve cloud computing security.

2.4 Summary

The abovementioned European studies, legislative initiatives and other efforts concerning the protection of critical (information) infrastructures show that network and information technologies become more and more vital for providing key services for a functioning society. Increasing complexity and interconnection of technical system and widespread use of information systems and network technologies lead to cross-border, cross-sectoral and even cyclic dependencies within critical infrastructures, resulting in new threat scenarios that require holistic approaches when it comes to critical infrastructure protection.

The main responsibility for secure operation of critical (information) infrastructures will probably stay with the main infrastructure operators themselves, regardless of what additional resources they rely on. Operators of critical (information) infrastructures relying on cloud computing resources as part of their systems should therefore aim at staying capable of assessing security risks and staying informed on security relevant incidents within services they use to support infrastructure operation. This means that enhanced transparency with regard to cloud computing security and enhanced capabilities for assessing security levels and tracing incidents and responsibilities within cloud environments used in critical infrastructure operation will increase with more wide-spread use of such services.

Use of cloud computing in critical infrastructures can improve security and availability of necessary information infrastructure resources used in critical infrastructure operation, as long as due attention is paid to risks and special security requirements coming along with cloud technologies.

The high level approaches planned by European legislators and the more detailed findings of the ENISA reports alike underline that technological approaches like the ones developed during the SECCRIT project which improve transparency and the possibility of real time views on cloud architectures and security relevant assets will become more and more relevant when it comes to outsourcing critical ICT services to cloud providers. Achieving a sufficient degree of transparency is indispensable to ensure that cloud resources used in the provision of critical (information) infrastructure services are under adequate control with regard to aspects like location, resilience and security measures in place at the various levels of a complex cloud infrastructure. Possibilities to gather live information about security are relevant as well as it is relevant to collect and store audit trail information in order to enable root cause analysis and thus clarify responsibilities, detect vulnerabilities and harden systems against future incidents. In the further course of the deliverable we therefore assess the current legal challenges stemming from the field of liability/evidence law and data protection law and show afterwards how we address them by technical means.

3 Legal Assessment

3.1 Evidence Law – the current legal situation

As already outlined in D2.2 Evidence law can be understood as the disclosing of facts which helps a party in a lawsuit to prove or disprove an issue in a lawsuit. For the SECCRIT project this means that it has to be delineated what facts need to be proven, what are recognized proofs and how technical support could be useful. At this point the deliberations made in D2.2 will be briefly sketched in order to permit a comprehensive understanding of cloud computing problems. Afterwards they are assessed in the light of the use cases.

3.1.1 In a nutshell

Evidence Law always comes as a second step into force, when the respective parties want to enforce their rights. It presupposes the material side. This means that within a lawsuit the court applies the provisions of the material law for the concrete case which it has to decide. The concrete regulations have to be subsumed and are therefore building the basis of the court decision. Contrary to criminal law, where the court itself determines the facts, civil law cases are characterized by the fact that the respective parties have to provide the proofs.

In practice it is thus difficult to find out the true circumstances of the case, as the parties are presenting it differently in order to influence the outcome of the process. Eventually evidence law has the purpose to permit finding out what truly happened and to help the court to determine the real facts which it has to subsume under the provision of the material law.

A lawsuit usually takes place for the enforcement of subjective laws. The legal action can have different shapes. The plaintiff can require a payment, restitution, injunction, and so on in terms of a performance action as well as declaratory actions and actions wherein legal relationships are modified by a judgement. However, the outcome of the proceeding depends on the proofs being provided by the parties of the lawsuit, respectively the plaintiff and the defendant. The plaintiff has to prove the facts on which his application is based on, whereas the defendant bears the burden of proof for the eliminating facts. This means in particular that the plaintiff has to prove the contract, the fault, the damage and the causal link between damage and fault.[23] The defendant in turn is responsible for proving the default, in particular that he didn't act negligent or intentionally and that also the persons he used to fulfil his duty didn't either act negligently or intentionally, as he is as well responsible for their behaviour.[24] The process considerations are consequently closely linked to the liability situation and in particular to the material side, as they are attributing, according to the specific claim, the legal consequence. Besides the general claim for damage, specific contracts have their own provisions leading for example to different limitation rules.

Liability enforcements depend on the fact that a damage occurred due to a negligent or intentional behaviour. In contract relationships the damage has to be committed because of a breach of duty. Therefore, the contract clauses need to be studied very carefully in order to permit the interpretation of the desired duty. After having clarified what the different parties actually owe each other, it has to be specified if the deviation from the owed duty has been committed intentionally or negligently. Failing to exercise reasonable care besides intentional acting leads from a material perspective to a compensation for damage. However, within the process constellation, the fact that it materially would lead to a compensation does not automatically

[23] S. Palandt/Heinrichs, section 280, recital 34.

[24] Palandt/Bassenge, section 280, recital 35.

mean that the plaintiff will get his damages compensated directly, it depends indeed on the proofs being provided by the respective party. This means that in the respective lawsuit, the behaviour of the plaintiff and the defendant are decisive. As substantiated as the claim of the plaintiff is, as substantiated the defendant needs to react. The substantiation content therefore depends on the statement of the respective other party. He can either admit or deny the fact. If the burden of producing evidence party asserts general facts without proofs, then the other party can strictly deny. A simple denial is, however, not sufficient in cases where the adverse party, in that case the plaintiff, provides explicit proofs in the beginning. The defendant is then obliged to plead more substantially. If he fails to substantiate it sufficiently, the claim of the plaintiff will succeed. If facts remain unclear (a so called non-liquet-situation) the decision of the court is based on the burden of proof. This means that the party, who had the burden of proof, will lose the lawsuit. This would mean for the plaintiff that the claim is rejected and for the defendant that the claim of the plaintiff is accepted. The respective party would therefore loose the case.

Facts which need to be proven are those which are disputed and important for the outcome of the lawsuit. Facts which are not necessary for the basis of the claim do not need to be proven. This also counts for obvious facts. The material side determines which facts are necessary to prove. The party which needs to prove facts has to convince the court about the alleged fact. The other party in contrast has to contest the evidence in a way that the court has now in turn reasonable doubts about the original proven fact.

3.1.1.1 *Consideration of evidence*

The court applies the principle of free consideration. This means that it has to decide itself if the disputed fact is true or not. The prima-facie-evidence can also be helpful for the court in situations where a typical course of event is given. The prima-facie-evidence constitutes a simplification of rules concerning the taking of evidence. In these cases, the court can deduct from a certain fact to another fact because of the experience of life. This is typically the case for causal circumstances and for the default. The party must prove in these cases only the facts which due to the experience of life result in the concrete fact of the material side. The legal conviction of the court is then gained by general experience. The adverse party, in contrast, can easily disprove it by pleading why in this particular case the experience of life is not valuable. The other party for which the prima-facie-evidence is advantageous has then to prove the respective fact with other proofs.

3.1.1.2 *Accepted proofs*

Facts can be proven by legal inspection, witness, expertise evidence, documentary evidence and the interrogation of a party.

The legal inspection comprehends every way of perception, like seeing, hearing, smelling, tasting and touching. The court has to perceive the facts itself. The witness proof, in contrast, is a very unreliable proof as it depends on the subjective perception of a person. Moreover, the neutrality of witnesses is often limited. The witness has to report the facts which he/she has observed in the past. The expert evidence in turn is important for areas where the court does not have the necessary competence and is confronted to questions which are not of legal nature. Due to his specific know-how, the expert helps the court to determine the true facts concerning the concrete case and transmits knowledge about facts and abstract general experience in that field. The documentary evidence is the most reliable proof as it gives a first indication of the respective fact. The other party in contrast would need substantiated proofs to refute this first given conviction of the truthfulness of the fact. Another possible proof is the interrogation of a party, which is as the parties are not neutral a subsidiary proof.

Especially for the SECCRIT project it will be interesting to classify which category of proof covers audit trails and how they could be recognized. Audit trails could permit to detect any deviation from normality and could then be used in court in order to show a fault and a negligent behaviour if what has caused the fault has also been recorded. Consequently, a continuous monitoring of the system could be valuable for evidence gathering. It must, however, be ensured that audit trails are not falsified and that they originate from the author. In the further course of the deliverable it has to be clarified how this could be achieved, depending especially on the legal conditions of the demo case countries.

3.1.1.3 *Electronic proofs*

Since within the SECCRIT project potential proofs are mainly of electronic nature, we need to evaluate how this type of evidence can be classified within the existing proof categories.

Such technical proofs could especially be subject to explicit European regulations. Electronic proofs could be falling under the provisions of the European directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The European directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures regulates the use of electronic signatures. As the directive is not directly legally applicable, all Member States are obliged to implement it into their respective national laws. The directive has the objective to facilitate the use of electronic documents and to guarantee their acceptance equal to written documents. The directive distinguishes between two different types of signatures: the electronic signature and the advanced electronic signature. Art. 5 of the directive 1999/93/EC on a Community framework for electronic signatures ensures therefore that “advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device” have the same legal value as handwritten signatures and are “admissible as evidence in legal proceedings”. The legal assessment of the electronic document therefore depends on the specific national evidence law and on how this type of evidence is considered within the respective national system. For example, it may differ between the formal acceptance of that proof in a way that the judge can “trust” directly the fact that the document has been produced by the author and has not been modified until it reached the addressee. Concerning the “material” content of the document, the court could be totally free in its interpretation in the meaning, that it could either believe in what has been electronically signed or not. Consequently, it will have to be analysed how the legal system the respective SECCRIT demo partner is subject to considers the evidence. The directive regulates, however, only the use of electronic documents and states that these are equal to handwritten signatures. The technical proofs envisaged by the SECCRIT project could need to be signed in order to be accepted in court. However, this depends on the legal evaluation of such signatures in the respective demo case countries. The next section is therefore dealing with the question how evidence law works within the countries where the demo cases take place and how proofs are recognized there in court. It further on concentrates on how the directive 1999/93/EC has been implemented into national Spanish and Finish law and how electronic signatures are accepted. Depending on how the proofs are recognized and judicially interpreted, such electronic signatures might not be needed if other possible proofs could be useful and could as well permit the recognition of these tools and their content in such a way that this facilitates the outcome of the process and the decision of the judge.

3.2 Evidence Law in Finland

The finish legal system is based on the Scandinavian and European tradition. The Code of Judicial Procedure, which is from 1734 and has been modified in the 20th century, regulates justice and procedural law. Especially, German private law discussions and theories have influenced the Finish Contracts Act[25].[26]

Statutes for evidence are regulated in Chapter 17 of the Finish Civil Procedural Code with the proceedings for the introduction of evidence and the substantive law of evidence, including regulations on the means, significance and the burden of proof. Inspection and written evidence are acceptable means of evidence.

Evidence law in Finland is also following the above described principle that within lawsuits the parties of the dispute have to provide the evidence and that the court is afterwards free to find the correct material result. The court is not bound by law.[27] In chapter 17, paragraph 1 of the Procedural Code it is stated that, "in cases of a dispute the plaintiff shall prove those facts which support his demands" and in cases were the defendant presents a matter to his advantage he must confirm it with evidence. The plaintiff has to produce substantiation as a basis for his action and the defendant needs to present opposing facts.[28] He also needs to provide sufficient evidence, Chapter 17, paragraph 8 of the Procedural Code. The free evaluation of evidence does not mean that the decision which one court makes is binding for a subsequent process. If, however, the party wishes to achieve probative value it needs to present the material and the judgement from an earlier case in new legal proceedings. This anticipates that in future proceedings the court will probably come to the same conclusion.[29] The court recognizes the relevant legal norms and applies them on its own initiative. The probative value of written evidence is defined by the free evaluation of documentary proof. The document is recognized as authentic until otherwise proven. The statement made by an expert is evaluated on the basis of the free evaluation of evidence.[30] The court often follows their statements due to their experience. There are no limits concerning judicial inspections.

Further on, the parties have to prove their demand to the satisfaction of the court. They have two possibilities: either they choose which evidence they want to provide in court or the court's assessment is free, i.e., it is not bound by law and that the purpose is to find out the materially correct result.[31] Finland has adopted the principle of free evaluation of evidence. In the Code it is stated that after the facts are considered carefully, the court should decide what is to be considered as truth.[32] This means especially for electronic documents, which are relevant for the

[25] In English: http://www.finlex.fi/en/laki/kaannokset/1929/en19290228.pdf

[26] Zalesinska, Civil contracts in Finnish legal systems with special consideration of electronic contracts Studia Erasmiana Wratislaviensia Acta Studentium, M. Sadowski, P. Szymaniec, E. Bojek (red.), Wrocław, 2009 r., p. 261, 263.

[27] DG ENTR/04/68 Finland, p. 2.

[28] Laukkanen, The law of Evidence in the Finnish Judicial System in The Law of Evidence in the European Union, p.118.

[29] Laukkanen, The law of Evidence in the Finnish Judicial System in The Law of Evidence in the European Union, p.121.

[30] Laukkanen, The law of Evidence in the Finnish Judicial System in The Law of Evidence in the European Union, p.130.

[31] Zalesinska, Civil contracts in Finnish legal systems with special consideration of electronic contracts Studia Erasmiana Wratislaviensia Acta Studentium, M. Sadowski, P. Szymaniec, E. Bojek (red.), Wrocław, 2009 r., p. 261, 268.

[32] Code in English: http://www.finlex.fi/en/laki/kaannokset/1734/en17340004.pdf; chapter 17 Section 2 (1).

SECCRIT project, that they are as valid as a paper document or a testimony of a witness.[33] The burden of proof in Finland lies with the party which is claiming damages. For example, the contractual obligation needs to be proven by the plaintiff in the meaning that a valid contract is given. The court is, however, free to interpret the contract and the obligations of it.[34]

3.2.1 Electronic Signatures

As European directives need to be implemented into national law, Finland is realizing this through amendments to various acts of national legislation.[35] The directive 1999/93/EC of the Community framework for electronic signatures by Electronic Signature Act was implemented in Finland on 1st February 2003. It specifies the types of electronic signatures and distinguishes between the electronic signature and the advanced electronic signature. The latter one can be certified by a third party. Signatures in electronic form are accepted by advanced electronic signatures which means, that a qualified certificates, created by a secure signature creation device, have the same legal effect as handwritten signatures and are admissible as evidence in legal proceedings. Because in Finland the courts are free to assess all evidence, electronic signatures are accepted without restrictions.[36] Such electronic documents are thus generally accepted without objections.

3.2.2 Electronic Proof

Audit trails could be used as evidence in Finland. As Finland has adopted the principle of free evaluation of evidence and the court should decide itself what is to be considered as truth, it is not necessary to provide audit trails with electronic signatures. An expert evidence as well as legal inspection could permit to assess the content of a technical document, respectively the audit trail. The court could afterwards decide if it wants to trust the content and thinks that this is true. Based on this, the court will provide its judgment. The expert will help the court to assess the content of the technical document, as the court might not have the knowledge to understand the meaning of it properly. Especially the non-falsification of the technical proof will be subject of the expert report as the expert needs to comment on the trustworthiness of the technical document. Therefore, the technologies established within the SECCRIT project which are focused on collecting evidence are useful, as the documents can be used for determining fault and default. In Chapter 5 it will be legally evaluated if and how the technologies developed are useable for evidence gathering.

3.3 Evidence Law in Spain

In Spain, provisions concerning proofs are defined in the Civil Code which determines the admission of the proofs and the LEY de Enjuiciamiento Civil, L.E.C. which determines the procedure of the acting measures. The court makes the decision according to the codified legislation and not by judicial decisions, Article 1 of the Spanish Civil Code.[37] This means that the "sources of Spanish laws are laws, customs and the general principles of law" and that case law only complements these sources. The parties must disclose the facts in front of the court. There is no general rule what documentary evidence has to be disclosed. The courts can order the

[33] Zalesinska, Civil contracts in Finnish legal systems with special consideration of electronic contracts Studia Erasmiana Wratislaviensia Acta Studentium, M. Sadowski, P. Szymaniec, E. Bojek (red.), Wrocław, 2009 r., p. 261, 268.
[34] DG ENTR/04/68, Finland, p. 5.
[35] DG ENTR/04/68 Finland, p. 1.
[36] DG ENTR/04/68, Finland, p. 2.
[37] DG ENTR/04/68, Spain, p. 2.

disclosure of documents by the parties itself or by third parties on the request of one of the parties, if the relevance is justified and there is no other possibility to obtain the document.[38] Concerning expert evidence this is appointed by the parties or by the court on the request of at least one of the parties.[39] The expert must provide independent opinions and disclose his assessment. The burden of proof lies with the party which alleges the fact and wants to get a certain effect related to the fact.[40] This means, that the party which is claiming an action has to prove the facts giving rise to the claim whereas the defendant is responsible for proving the eliminating facts. The plaintiff has to prove a misbehaviour, in a negligent or wilful manner, the suffered damage and the causal link between the negligent conduct and the damage. The evidence is mostly judged according to the rules of reasonable assessment which is called “reglas de la sana critica”, which means that the court is free to consider whether or not the evidence is sufficient to convince the court about the existence of a disputed fact.[41] Private documents are accepted in court just as public documents which are considered as incontrovertible evidence of the fact documented in it. If, however, a document is disputed concerning its authenticity the court is assessing it freely, according to the rules of reasonable assessment.[42] The above described prima-facie-evidence is also accepted in Spain, the uncertain fact (hecho presunto) is considered as true if it is linked to another certain fact (hecho cierto).[43] Accepted evidence in Spain is, as summarized above, the examination of the parties, documents, the expert’s report, the inspection of the court and the witness, recorded words, sound and images.[44] The list of forms of evidence is however not final (numerus clausus), meaning the court can use any form of evidence that could be necessary for the decision.[45] In Spain it is not foreseen that business secrets are protected and do not have to be disclosed in court.[46] Contributory negligence is also recognized in Spain.[47]

3.3.1 Electronic Signatures

The directive 1999/93/EC on a Community framework for electronic signatures has been implemented in Spain by Law 59/2003 of 19th December 2003. It defines the electronic signature as a “set of data in electronic format, sent or associated with other data, that can be used as a means of identifying the signatory”. The electronic signature therefore permits the identification of a person. In contrast to finish law, Spanish law recognizes three different types of signatures which are the electronic signature, the advanced electronic signature and the recognized signature based on a qualified certificate. Whereas the electronic signature only can be used to identify someone, the advanced signature is based on an electronic certification which not only

[38] Alvaro Mendiola; http://uk.practicallaw.com/7-523-2553
[39] Alvaro Mendiola; http://uk.practicallaw.com/7-523-2553
[40] Jesus Almoguera et.al., p. 9; http://ec.europa.eu/competition/antitrust/actionsdamages/national_reports/spain_en.pdf
[41] Jesus Almoguera et.al., p. 9; http://ec.europa.eu/competition/antitrust/actionsdamages/national_reports/spain_en.pdf
[42] Jesus Almoguera et.al., p. 10; http://ec.europa.eu/competition/antitrust/actionsdamages/national_reports/spain_en.pdf
[43] Jesus Almoguera et.al., p. 10; http://ec.europa.eu/competition/antitrust/actionsdamages/national_reports/spain_en.pdf
[44] Jesus Almoguera et.al., p. 10f; http://ec.europa.eu/competition/antitrust/actionsdamages/national_reports/spain_en.pdf
[45] Jesus Almoguera et.al., p. 11; http://ec.europa.eu/competition/antitrust/actionsdamages/national_reports/spain_en.pdf
[46] Jesus Almoguera et.al., p. 12; http://ec.europa.eu/competition/antitrust/actionsdamages/national_reports/spain_en.pdf
[47] Jesus Almoguera et.al., p. 16; http://ec.europa.eu/competition/antitrust/actionsdamages/national_reports/spain_en.pdf

permits the identification of the person who signed the document but also the detection of any other change in the document that has been signed.[48] The recognized electronic signature corresponds to the advanced electronic signature of Art. 2 of the Directive 1999/93/EC. It is based on a recognized certificate, is linked to the signatory, is capable to identify the signatory, is created using means that the signatory can maintain under his sole control and is linked to the data to which it relates in such a manner that any subsequent change is detectable. Under Spanish law, the electronic signature in respect of electronic documents is recognized just the same as a written signature on physical documents. This means that the electronic signature has the same legal value as a written document.[49] Electronic documents are documents containing the data signed electronically and drafted in an electronic support.[50] An electronic document, signed in that manner is according to Article 3.8 of Law 59/2003 admissible as evidence.

3.3.2 Electronic Proof

Since in Spain a numerus clausus of accepted proofs does not exist and any form of evidence which could be necessary for the decision can be used, audit trails could be directly accepted as a proof and the court can decide freely if it trusts the content. Additionally, an expert evidence and legal inspection can permit to determine the content of such log files. The court is then free to consider whether or not the evidence is sufficient. In this way the developed technologies could be useful in order to permit the gathering of evidence, which could be used for the decision of the court with regard to disputed facts.

3.4 Interim Result

The respective national laws of the demo case countries recognize the use of electronic documents. Since in both countries the court applies the free judicial evaluation, evidence produced by SECCRIT technologies can be recognized in court. They do not need to be electronically signed since an expert and legal inspection could as well assess their value and truthfulness. The expert will especially have to analyse the truthfulness and its content.

3.5 Material Side within cloud computing cases

After having evaluated the national provisions we will concentrate on the material and procedural side of liability and evidence law. Before the process-side (s. D2.2) can be analysed and mapped to cloud computing cases, the material side needs to be clarified. The cloud user will only be indemnified if a legal basis exist, a breach of duty was committed and the user had a damage due to this breach of duty. The legal basis could either be a contract or a legally codified one like tort regulations. Within the SECCRIT project we will however only concentrate on contractual claims as the cloud user and the provider relationship is normally based on a contract.

3.5.1.1 *Legal qualification of the cloud contract*

At this point the cloud computing contract needs to be qualified. This permits to recognize a fault, as the legal qualification enables to really identify an owed duty and thus the deviation of it. Additionally, the qualification also permits in a further step an attribution of the burden of proof to each debtor of the specific duty.

[48] DG ENTR/04/68, Spain, p. 3.
[49] DG ENTR/04/68, Spain, p. 3.
[50] DG ENTR/04/68, Spain, p. 3.

Generally speaking, no specific cloud legislation and thus legally anchored contract exist. The same applies to cloud computing case law, as at least no cloud-specific case with a respective cloud-based fault could be reported.[51] Consequently, cloud computing contracts are subject to specific national general laws, which apply to all kind of different subjects.

As cloud computing services are often composed it is quite difficult to subsume them under one single defined type of contract. Such mixed contracts are legally treated differently.[52] Some legal scholars are firstly determining which the main duty of the contract is and only apply the respective provisions.[53] Others are distinguishing between the different duties of the contract and are applying the respective provisions applicable for the defined type of contract matching the specific performance.[54]

A first starting point for classifying cloud contracts could be the legal discussions concerning the already existing case-law specific attribution to application-provision, access-provision, and outsourcing contracts.[55] These models are mainly considered as lease contracts.[56] The difference to cloud computing contracts is however, that within the latter one, all data of the users are co-located within the same infrastructure and additionally a direct attribution to a physical hardware is not given. The tenant does not know on which server the data are located, as these can be stored individually or spread across different servers. Cloud computing also supports multiple tenants in contrast to outsourcing contracts, where the provider is only responsible for one single client. With respect to this, it is not possible to simply apply the case law assessments concerning application-provision, access-provision, and outsourcing contracts. An own legal assessment is therefore necessary as the specific characteristics of cloud computing could probably require a different qualification.

3.5.1.1.1 Cloud computing contract in different European countries

However, within this deliverable an own assessment on how cloud computing contracts are qualified, is not necessary, as the European commission already has produced a comparative study on cloud computing contracts, whereas the commission provides an overview about legislation in the different European countries concerning cloud computing.[57] The European Union or, respectively the commissioned firm DLA Piper, come to the conclusion that in some countries cloud computing contract are subject to the provisions for service contracts, work contracts, lease contracts or must be seen as so called “sui generis” contracts (these are contracts of their own, which do not fall under a certain predefined type of contract). In Spain and Finland, cloud computing contracts are qualified as service contracts.[58] The service contract is codified in Article 1,544 of the Spanish Civil Code[59]. The legal codification is, however, only an additional interpretation aid for the contract, especially for the circumstance that the contract is lacking specific clauses. Therefore, mainly the wording of the contract is the starting point for its interpretation. The cloud user’s interests must be represented in the contract. If the wording of the contract is not very clear, the intentions of the party need to be considered. Additionally, the

[51] DLA Piper UK LLP, prepared for the European Commission, p.26; they are referring that at least no case which had a cloud-specific fault could be reported.
[52] Mü/Ko-Thode, § 305, Rn.67, Palandt/Heinrichs, v. § 311 Rn. 24.
[53] Absorption theory, Lotmar, DER Arbeitsvertrag I, 1902, S. 176, 686ff.
[54] Combination theory, S.a. Palandt/Heinrichs,Vor § 311, Rn. 24.
[55] Schuster/Reichl, Cloud Computing & SaaS: Was sind die wirklich neuen Fragen? CR 2010, 38, 38.
[56] BGH MR 2007, 243. Pohle/Ammann, CR 2009, 273, 274; Schulz/Rosenkranz, ITRB 2009, 233.
[57] DLA Piper UK LLP, prepared for the European Commission.
[58] DLA Piper UK LLP, prepared for the European Commission, p. 28.
[59] http://www.elra.eu/wp-content/uploads/file/Spanish_Civil_Code_%28C%C3%B3digo_Civil%29%5B1%5D.pdf

legally codified provisions are taken into account. If, for example, the cloud contract does not have detailed provisions concerning a specific constellation the codified legally regulated provisions are applied. Therefore, at least for the assertion of the claim, the fact that a cloud computing contract has been concluded is sufficient to determine obligations and duties for the respective parties. They are forming the legal basis for the claim. For the cloud user it is mandatory that his interests are represented within the contract.

3.5.1.2 *Fault and default*

As the contract clauses are determining what the parties owe each other, they simultaneously permit to identify a breach of duty. Any deviation from duties owed could a breach of duty. The attribution of being indemnified depends, however, on further elements. It is therefore of particular importance for the cloud user to ensure that the performance of the provider is contractually fixed. After having identified the possible claims it has to be analysed what could be a possible fault of the cloud provider. Throughout the course of the project it turned out that the legally identified faults correspond to the cases specified in the anomaly detection/risk assessment vulnerability catalogue.

Determining a fault depends on the respective contractual obligation of a party. It has to be distinguished between what actually happened, respectively what was the cause, in particular an acting or failing to perform a certain act. Legally, it has to be clarified if it is a main performance or a secondary obligation.

Therefore, different constellations can be identified: The provider is contractually obliged (as a main performance) to provide a functioning system, which the user needs for his purposes. Besides, the provider is also responsible for protecting the user from any harm (secondary obligation).

If, for example, it comes to a non-availability of the system or a data leakage then this is a deviation from an owed obligation. The fact that this happened can be caused by an own acting (misconfiguration for example) or a failure to act, especially if security updates have not been installed. The nature of this cause can be for example viruses, hacker attacks, a misconfiguration, overload, breakdown and force majeure. In a further step it has then to be classified if these causes have been committed intentionally or negligently by the provider. Negligent means in this case that the obligor failed to exercise reasonable care. Default is assumed by law. This means that the defendant has the obligation to contradict this already assumed negligent/intentional behaviour. For this he requires adequate proofs.

Along these identified causes which could have caused a breach of duty like the non-availability or a data leakage of the system, it will be briefly elucidated what are the obligations of the provider. At this point it will be briefly sketched what would be in different constellations considered as negligent behaviour.

3.5.1.2.1 Causes

Besides the causes already listed in D2.2 which will be summarized in short, changes and or novel causes will be reported in more detail.

3.5.1.2.1.1 Virus

A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". The term "virus" is also commonly, but erroneously, used to refer to other types of malware. "Malware" encompasses computer viruses along with many other forms of malicious software, such as computer worms, ransomware, trojan horses, key loggers, rootkits, spyware, adware, malicious BHOs and other malicious software. The majority of active malware threats are actually trojans or worms rather than viruses.[60]

It turned out during the course of the project, that viruses can also cause severe damage within cloud based systems. However, it has to be distinguished which cloud system is affected. If infrastructure as a service (IaaS) is contractually owed, then the client can use this system on his own with his own software which can indeed be affected by a virus. It will be the customer himself who will have to clear the virus, as the cloud provider is only responsible for the IaaS system. In these cases the provider only needs to provide the IaaS system, therefore this is the duty which he owes to his client. If a virus, however, attacks the IaaS platform, then the cloud provider could possibly in case of a damage sue the customer / cloud user if he acted negligently or intentionally. This is the case, if he failed to use common security measures.[61] In turn, if the IaaS-system itself is affected, and this can infest the client’s system, it will be the client who can in case of a damage sue the cloud provider. This is generally not a probable case. However, recently, time channel attacks were reported concerning Amazon EC2.[62]
For platform-as-a-service systems (PaaS), virus attacks are also imaginable, since viruses can actively influence program code in a negative manner which is then executed in the cloud. Concerning software-as-a-service-platforms like, Dropbox it seems quite unlikely that something happens directly in the cloud system like a virus which spreads over the entire system.
The provider is in that senses obliged to protect his system adequately in order to avoid a virus attack.

3.5.1.2.1.2 Overload

Negligent behaviour would be given, if it comes to an overload and the system is not available or data gets lost. As overload situations can be avoided by one of the main characteristics of cloud computing, namely the use of other existing servers, the provider would be responsible in such a situation.[63]

3.5.1.2.1.3 Breakdown

The provider is generally responsible to undertake precautions at its best. Depending on the contract closed, this means, that he has the duty to protect his data centre from power blackouts and other possible failures and must secure it through technical attendance.[64]

[60] Aycock, Computer Viruses and Malware, p.2ff.
[61] Balaban/Pallas, InTeR 2013, 193, 197; Balaban/Pallas, DSRI Herbstakademie, p. 335.
[62] Ristenpart/Tromer/Shacham/Savage, Hey you, get off of my cloud:exploring information leakage in third-party compute clouds, proceeding CCS ’09 proceedings of the 16th ACM conference on Computer and communications security.
[63] Balaban/Pallas, InTeR 2013, 193, 197.
[64] S. D2.2.

3.5.1.2.1.4 Hacker Attack

Concerning hacker attacks, the provider should eliminate software-bugs as they enable hacker-attacks.[65] Moreover, adequate access control mechanisms in particular protection features like firewalls need to be used.[66]

3.5.1.2.1.5 Force Majeure

Responsibility in the context of force majeure cases is hardly given. However, if the provider can fall back on different locations thus ensure geo-redundancy by holding fall-back systems, he could indeed be made responsible for ceasing such an outsourcing on other servers in another country.
This, however, depends on what the respective parties have actually agreed on. If geo-redundancy was legally owed, the provider would in these cases be liable if he failed to outsource the specific data.

3.5.1.2.1.6 Technical defect

The provider has to perform all necessary measures to protect servers from any technical incidents. This implies also regular maintenance.[67] He is therefore responsible if he fails to use the appropriate measures in advance which could have prevented such technical defects.[68]

3.5.1.2.1.7 Misconfiguration of the system

Generally, the provider will be responsible for configuration errors. However, this does not only depend on the specific case, but also on the question if he failed to exercise reasonable care when the system was configured. If he did this according to state-of-the-art and it was not foreseeable that an error could occur, he would then not have acted negligently.

3.5.1.2.2 Summary

To sum up, it is considered that providers are acting negligently, if they use outdated technologies for IT-security.[69] Moreover, providers need to update their security software timely and regularly. Closing vulnerabilities as well as the use of firewalls is demanded by state-of-the-art practices that have to be considered as necessary duties for which the provider would be liable if he fails to make use of them. The provider is generally responsible if he fails to apply common security standards. He is, however, only responsible in cases where these security mechanisms could have prevented such causes, like in case of a hacker attack, viruses or technical defects. Furthermore, irrespective of security mechanisms, he will be responsible for overload situations and errors caused by misconfiguration.

[65] Wulf, CR 2004, S. 43 (48).
[66] Balaban/Pallas, InTeR 2013, 193, 196.
[67] Wulf, CR 2004, S. 43 (48).
[68] Wulf, CR 2004, S. 43 (48).
[69] Beucher/Utzerath, Cybersicherheit – Nationale und international Regulierungsinitiativen folgen für die IT-Compliance und die Haftungsmaßstäbe, MMR 2013, 362, 367.

3.5.1.3 *Liability for Sub-Contractors*

In case the cloud provider uses subcontractors to perform the duties owed to his customer, he is also responsible for their behaviour.[70] This also applies for subcontractors of subcontractors, either because the cloud user has given the cloud provider his consent concerning their use or because no consent was given and the provider acted negligently because he outsourced his duty to a third party without being authorized to do so by the cloud user.[71]

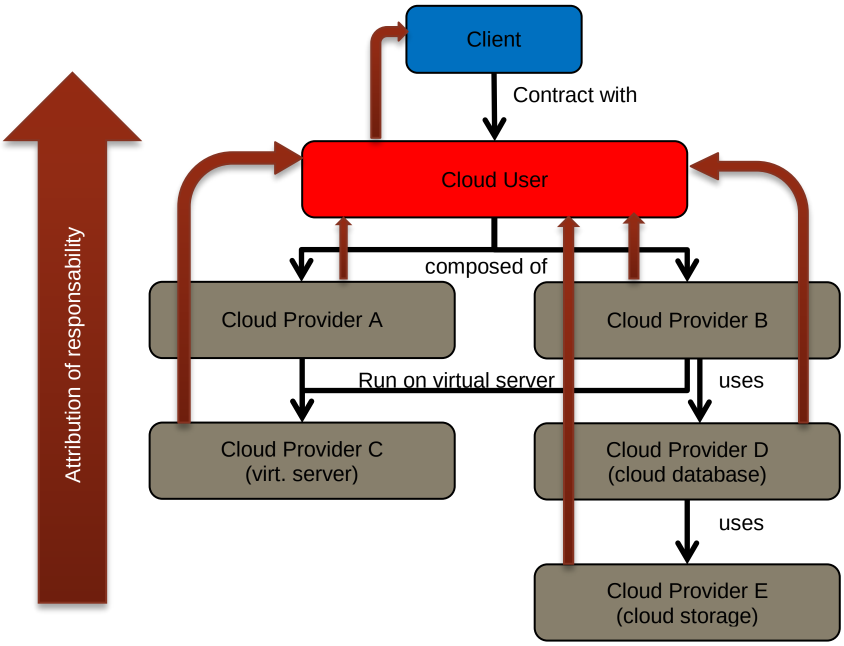

FIGURE 2: ATTRIBUTION OF RESPONSIBILITY IN COMPOSED SYSTEM

This figure illustrates the different liability constellations in composed systems, and the fact that there is an attribution of responsibility in the meaning that the cloud user is responsible for the behaviour of all persons he uses to perform his duty against his customer.

3.5.1.4 *NIS-Directive*

At this point, it should be elucidated if the NIS-Directive increases the liability. The NIS-directive (Network and Information Security Directive), as stated above, has been proposed by the European Commission in February 2013. The directive obliges member states to develop a national network and information strategy. In Art. 5 (2) of the NIS-Directive, the adoption of a national NIS cooperation plan which should comply a risk assessment, a definition of the roles

[70] Karger/Sarre p. 433; Söbbing, MMR 2008, book 5, S. XII, XIII bis XIV; Leupold/Glossner-Stögmüller, Münchener Anwaltshandbuch IT-Recht, part 5 Internationale Bezüge des IT-Rechts einschließlich Internationales Privatrecht, 2. edition 2011, recital 335.
[71] BGH 18.05.1995 – X ZR 114/93, WM 1995, 1457f; Palandt-Heinrichs, § 278, Recital 9.

and responsibilities of the various actors, a cooperation possibility which shall ensure prevention, detection, response, repair and recovery and modulated according to the alert level is required. Each member state has to designate a national NIS-authority who has to fulfil the requirements of the directive (Art. 6 NIS-Directive). Art.8-11 of the NIS-Directive obliges the ENISA to establish, together with standardization bodies and relevant stakeholders, technical directives and recommendations for the introduction of NIS-standards. Critical infrastructure operators and internet companies are obliged to take appropriate technical and organizational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. “Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimize the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems”, Art. 14. IT-Security needs to be fulfilled especially because the contractual partners need to respect the legal interests of each other. The obligation stemming from the NIS-directive to adopt a certain IT-Security Standard is not a new one as the already existing technical norms are recommended to be followed. These existing technical norms are used as a reference to determine if a company has exercised standard care and diligence. Following the state of the art is considered in court as a prima-facie-evidence in the meaning that the respective party did not act negligently. The adversary party can then disprove this by showing that despite following the state of the art no reasonable care was exercised. However this is going to be quite difficult as the state of the art already indicates a sufficient level of security.

As the previous legal situation had also foreseen to use at least common security standards which are not outdated, the NIS-directive will not lead to an aggravation of liability. However, existing technical standards will probably become more specified and especially sector-specific.[72]

3.6 Process side and cloud computing

In order to assess what necessary proofs the cloud user requires for being indemnified and to clarify insofar if the technologies developed within the SECCRIT project could be useful for this aim the process side will be elucidated in the light of cloud computing services.

For this, we present beside the use case in Section 1.2 two additional simplified cases which shall permit to identify the different evidence situations in relation to the Mirasys use case, the act of vandalism in the night. Especially differentiating the roles of the cloud user once as a plaintiff and once as a defendant will help to elucidate easier the current legal proving situation.

3.6.1 Constellations:

First Case: A cloud user (A) has a contract with a cloud provider (B), the latter commits a breach of duty and the cloud user suffers a damage. The cloud user wants to get his damages compensated, so he sues the cloud provider.

Second Case[73]: Cloud user (A) has a contract with a customer (C) and demands a cloud-based solution in fulfilment of the contract. He has for this a contract with the cloud provider (B). That

[72] Beucher, Utzerath: Cybersicherheit – Nationale und internationale Regulierungsinitiativen - Folgen für die IT-Compliance und die Haftungsmaßstäbe, MMR 2013, 367.

[73] This case is very simplified, we assume however that the fault occurred within the sphere of the provider and we are disregarding the fact that someone else committed a damage to property.

one commits a breach of duty (for example a non-record of video images) and it is the client of the cloud user who has a damage. C sues the cloud user. This case resembles the Mirasys Use Case Nr.1, as MetroSub contracts CitySec for the surveillance of the station. CitySec in turn contracts TenSYs Ltd. which is the provider. The case, however, is composed of other actors, s. case three.

Third Case: The act of vandalism in the night (Mirasys Case Nr.1): Just as the second case. MetroSub is the client, City Sec is the provider. The latter one has a contract with TenSYs Ltd., who contracts CloudCorp Ltd., a supplier of servers for data storage and processing and TelCom Ltd., a telecom operator for data communications. The difference with regard to the second case is that the cloud provider is providing a composed system and is using for this services from other providers.

3.6.1.1 *Evaluating the first Case:*

In the first case the cloud user needs to prove an existing contract or at least a legal basis for his claim, a breach of duty, his damage and the causal link between damage and breach of duty.

Proving the contract and his damage won't raise any major problems to the cloud user. With the document proof the legal basis could be proven. As already depicted in 3.5.1.2 the breach of duty can, for example, be a failure, a non-functioning of the system but also loss of the data. These causes can be proven by legal inspection, expert evidence and/or a document. For the cloud user this does not cause any particular difficulties, however, now the provider has the possibility to prove that he did not act negligently[74]. As these facts lie in the realm of the provider and the cloud user has no inside view in cloud-specific ongoings, the cloud provider could in particular as well prove with (electronic) documents that indeed a failure of the system was given but this was not due to a wrong behaviour of him. For instance, he could show by electronic documents that he used the recommended security updates and therefore exercised reasonable care as expected. This document could indicate that nothing particularly happened, that he used all demanded security measures. Further on he could show with such a document that the cause of the failure cannot stem from his realm because nothing particular has been reported.

As the civil process resembles a "ping pong game" it will now be the cloud user who will have to refute the proofs of the provider. For this he has the means of legal inspection, documents, witness and expert evidence.

3.6.1.1.1 Legal inspection

Legal inspection will in this particular case not be a useful proof as the cloud computing contract is a continuing obligation and especially in case of a failure the particular situation will be a past incident so the court cannot notice failure by own perception. Legal inspection can additionally be used for the evaluation of another proof, like documents for example.

3.6.1.1.2 Witness

As the proofs of what actually caused the failure or data leakage etc., if they have been saved, can only be in the realm of the cloud provider, as he has the data sovereignty, it will be very difficult for the cloud user to find a witness who could disprove that the provider acted negligent. At least this witness will very likely be an employee of the cloud provider. It is hardly conceivable that an employee of the cloud provider would testify against his employer, at least it will be

[74] We estimate that he is not acting intentionally.

difficult for the cloud user to actually find the one who acted negligently. To sum up it will be very difficult for the user to actually find a witness who could testify that the provider acted negligent.

3.6.1.1.3 Document Evidence

Concerning the document proof the same applies as to the witness document. All documents which could indicate what the provider used as security updates etc. are internal processes. The user only sees his application mask. He therefore has no inside view in what the provider is doing in particular he has no inside view in the clouds internal processes. As a consequence the cloud user cannot reproduce what has caused the failure. The documents he receives only concern his own web interface. Internal data processing mechanisms are not disclosed to him, which would be important for him in order to permit him to really assess what the nature of possible failures is.

3.6.1.1.4 Expert evidence

Generally speaking, expert evidences are a good modality to reproduce what actually happened. Especially in offline cases they are very useful to the process parties. However, concerning cloud computing cases it is very difficult to actually retrace what caused the failure.[75] Expert evidence can be used for assessing the documents provided by the cloud provider and indicating what the provider did. This means, however, that these documents are not neutral as they are stemming from the providers side. Those documents can therefore show what security updates and which processes the provider has induced but they cannot guarantee their integrity. Without any supplemental proof from another neutral instance it is difficult to assess the truthfulness of such documents.

3.6.1.1.5 Summary

In the first case the cloud user will lose the lawsuit as he is in lack of possible useable proofs to disprove the negligent acting of the provider and thus unable to contradict the non-default of the provider.

3.6.1.2 *Evaluating the Second Case:*

In this case the cloud user is the defendant and he is sued by his client. For the client it is very easy to prove an existing contract, a breach of duty, a damage and the causal link between damage and breach of duty. Taking the Mirasys use case as an example for such a constellation, the security service provider CitySec would be the cloud user, MetroSub would be the client. TenSys is the cloud provider. CitySec is therefore the defendant. For MetroSub it is very easy to prove that the metro station was vandalized, by documents, legal inspection, witness proof etc. and it will now be on the cloud user to prove that he did not act negligent as his duty was to supervise and protect the station. As the cloud user relied on the provider in order to perform the duty he owes to his client (the video images are stored in the cloud), the cloud user is in return also responsible for any acts or omittances of the cloud provider. It is therefore necessary to prove that neither him nor the cloud provider acted negligently.

It is, however, necessary to take a closer look on what was causal for the damage of the station. Assuming that the damage is connected to the cloud computing system, it could have either been caused by a fault of the cloud user, if he made for example some passwords accessible, or by the provider himself (see section 3.5.1.2.). The possible fault and defaults are therefore increasing as

[75] Wicker, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? – Relevante Haftungsfragen in der Cloud, MMR 2014, 715, 717.

also the cloud user himself could have been responsible for a failure, or a loss of the data leading to a damage of his client, as the data are necessary for the fulfilment of the contract. Fault, in this case, could be either an acting or a non-acting. The cloud user will especially need to prove that he himself did not do something wrong as the major cloud computing service is provided by the cloud provider. This means that this second case actually contains also the user/provider evidence problems of the first case, since the cloud user indirectly needs to disprove a fault in the realm of the provider. The problem originates from the fact, that the provider could indeed help the cloud user and show like above that he did not commit any wrongdoing. It is very unlikely that he will admit negligent behaviour. As the default is however assumed, this has for the cloud user the consequence that he also needs to prove that he himself did not do something wrong, as the indication of a damage alone is sufficient enough for assuming a wrongful in particular a negligent behaviour. Even the help of the cloud provider by showing, that documents did not record any particular failure or negligence does not disprove that the user himself was responsible for the fault.

Proving non-negligence of the provider requires the “help” of the provider. It is, indeed, in the interest of the provider, to prove that the damage was not caused in his realm since this would permit the cloud user to sue the provider once it is proven that the fault lies in the realm of the provider. This would have the consequence that the cloud user would lose the lawsuit against his client, as he is responsible for the behaviour of the provider. He will therefore have to compensate the damages suffered by the client and could in return take recourse on the provider. Legally it will be highly recommended to have a third party notice, in the meaning that the provider adheres the process, as the first decision of the court would be legally binding for a subsequent process in such constellations. If in the first process therefore it is proven that the fault is due to a breach of duty of the provider the third party notice would permit the cloud user in a subsequent process to get the damages he had to pay back from the provider as it is already proven that a breach of duty was committed by the provider.

Again it is, however, highly difficult to prove the providers fault. The cloud user is in this constellation in a highly precarious situation: Even if he somehow manages to prove the providers fault he will lose the lawsuit. Getting back the payed damage because he needs to refund his client along with the process costs depends also on the solvency and the possible enforcement against his contractual partner, the cloud provider. It is not very unlikely that the provider could be bankrupt and the user does have a title on whose basis the execution can be levied but this is valueless if he is only one creditor among others. This means that proving the negligence of the provider does not mean that it releases him from paying the damage to his client, as he is the contractual partner of the latter one and the client has the claim against him.

The cloud user is therefore interested in proving that neither he himself nor the provider has committed a breach of duty.

Proving that it was not the provider’s fault requires the help of the latter one. Proving the provider’s fault and afterwards suing the provider brings the cloud user in the same situation as in the first case without a third party notice. A witness proof won’t help the cloud user, s. above, section 3.6.1.1.3. In return the provider could indeed provide a witness like an employee explaining that he did not act negligently. In addition with other proofs like documents for example, it could indeed be proven that the provider exercised the reasonable care.

This however leads to the fact, that the provider, respectively the cloud user in this second case as he is the party of the process can disprove a negligent behaviour of the provider. For the cloud user now it still remains to prove that he himself did not act negligent. Proving that it was, however, the provider is hardly feasible, as proofs are kept in the realm of the provider and the cloud user has no opportunities to proof a contrary fact (see first case). This means that the presumed fault remains concerning the cloud user. He will have to disprove a possible negligent behaviour of himself. This is highly difficult for him as it also consists a negative proof in the meaning that he did not do something wrong. For the cloud user it is therefore important that he manages to prove that the provider committed a fault, as he would lose the first case but he could win with a third part notice the second lawsuit against the provider, as in the decision of the first case is legally binding for the second one. This means that it is of high importance that the user proves the providers fault in order to not have to prove his possible own fault, as such a proving situation is highly difficult for him.

In order to illustrate this problem in more detail again the following proofs are analysed concerning their practicability for the user in a respective lawsuit:

3.6.1.2.1 Legal Inspection

Legal inspection would again imply an own perception which is only plausible in combination with a document.

3.6.1.2.2 Witness

A witness could testify that the cloud user has exercised reasonable care. It is however mainly difficult for witnesses to testify about facts concerning an activity which the cloud user has not done, like for example making passwords accessible to another person. Further on, it is highly unlikely that the witness proof alone can be sufficient to disprove a possible default of the cloud user, as the fact that a vandalism happened is all alone enough to prove that a default is given. The default is assumed and the cloud user must disprove it by proving that it didn't occurred in his (and the providers) realm. As there is an assumption that it is his fault, this is highly difficult.

3.6.1.2.3 Document

Proving that the user himself did not act negligently with a document seems quite difficult as it will only concern his own internal application mask. Only for this he could record electronic documents. In this vandalism case it appears that this happened due to a non-record of video images within the cloud, in particular a cloud-specific reason. As the cloud provider can easily disprove negligent behaviour (see first case) it is questionable how the cloud user could collect electronic documents proving that he himself did not do something improper. Main problem therefore is that the negligent behaviour actually lies in the realm of the provider (see case description), this is however legally not provable with the consequence that the provider is not liable. As the assumption of default remains concerning the cloud user, that one requires proofs for proving reasonable care. A document proof can, however, not disprove all possible acts or ommitances which could have led to the occurred vandalism. The fact that this happened makes it very probable that someone (either the provider or the user) did not exercised reasonable care. In contrast to the provider who is in a good proving situation, since the data is kept within his realm, the cloud user has no possibilities to refute this probability of a negligent behaviour. It still remains unclear and proofs like documents cannot rebut all possible negligent behaviours. In such a situation, the cloud user, as he is responsible for proving the default, will lose the lawsuit.[76]

[76] At least in the case that no other third party has for example destroyed the cameras and the user shows with respective video image the situation where that third party has destroyed the camera.

3.6.1.2.4 Expert Evidence

Expert evidence is generally helpful. However, in this constellation it will again be difficult to find out the real fault, as only cloud internal documents exist which might not be complete and might not have recorded the actual fault. Moreover, it is difficult for an expert to disprove a possible of the cloud user himself. The fact, that the station was vandalized is sufficient for proving the fault, as a damage occurred which the contractual partner was obliged to prevent.[77] The user has then to prove the cause of the damage and that he is not responsible for this. It is also sufficient that he proves the most probable cause of the damage and the fact that he is surely not responsible for this.[78] If the cause cannot be found he will have to prove that he observed all type of care.[79] If several potential causes of the fault are probable, he will need the proof of exoneration for each cause.[80] The expert evidence will, in this constellation, probably not be helpful, as it is indeed difficult to retrace from which realm the problem originated.

3.6.1.2.5 Summary Second Case

In the second case, the cloud user as the defendant will lose the lawsuit against his client, because the provider will again disprove a possible own fault. The user will then fail to disprove his own fault. The cloud user will have to pay his client the damage of the vandalized station.

3.6.2 Evaluating the Third Case

This case summarizes the legal problems of the first and the second case. This means that the user is in the proving situation of the first case as he will have to prove the provider’s fault and he is simultaneously in an evidence situation similar to the second case as he will have to disprove an own wrongful behaviour. Additionally, more parties are involved and he will also have to take a stand concerning the other providers. Proving that it was someone else than him who is responsible for the cause of the damage and proving that he exercised all reasonable care would permit him to lose the lawsuit against MetroSub and win the second one against the provider who committed the already proven fault.

In this case again the user is interested in proving that one of the providers is responsible for the fault. This implies also that he manages to prove a possible fault of the persons whom the provider uses in order to perform his duty against his client, the cloud user.[81] The cloud user CitySec will need proofs against TenSYs Ltd., CloudCorp Ltd. and/or TelCom Ltd. The difference between this case and the second case is that especially in a composed system it becomes even more difficult to retrace a possible fault, as more actors are operating and the fault can have occurred in different realms. Again, the cloud user suffers from a lack of inside views and can hardly prove that one of the providers is indeed responsible for the damages occurred.

3.6.2.1 *Legal inspection*

Legal inspection will require other proofs in order to permit an own perception.

[77] Hamm NJW-RR 89, 468.
[78] BGH 116, 334, 337.
[79] BGH NJW 65, 1585.
[80] BGH NJW 80, 2187.
[81] Balaban/Pallas, InTer 4/13, 193ff; Balaban/Pallas, DSRI Herbstakademie, 335ff.

3.6.2.2 *Witness*

Proving the fault of the provider and also a possible fault of the provider of the providers would imply that employees of the providers testify against their employer which is hardly conceivable. Still the cloud user could use the witness proof to prove that he himself exercised reasonable care. Here again, this witness would need to testify about negative facts, which is generally extremely difficult. Additionally, the fact that a damage occurred already implies a given fault, which in turn has to be disproven by the user as the defendant. As the difference between the user and the provider lies in the fact that the possible proofs are all in the realm of the provider, the providers can all in turn exonerate whereas the user still remains responsible for disproving an own fault. He will hardly manage to prove the fault of someone else by witness proof as the damage alone is sufficient for proving the fault. He would need additional proofs for substantiating this.

3.6.2.3 *Document*

Here again, concerning the provider and the provider of the providers fault, this will require neutral proofs which the cloud user does not have as documents are in the realm of the providers and they will hardly provide them in order to not be sued by the user afterwards. Documents showing that the user has exercised reasonable care could be useful but again, if the providers exonerate themselves and the fact that a damage occurred alone is sufficient to provide the fault, the user will still have to disprove an own possible fault. The user therefore requires documents which can show that either what providers provide is not truthful or the most probable cause which is apparent by own documents. The current legal position does not permit him to proceed like this.

3.6.2.4 *Expert Evidence*

An expert will primarily be focused on evaluating the documents provided by the providers. He will have to take position concerning the non-falsification of these documents. However it will be quite difficult for him to really assess what actually went wrong within the system, especially in a composed system where several actors could have committed a breach of duty. He will therefore have to evaluate the behaviour of all the providers in order to deduce the true cause. This implies that he has to take in mind all possible causes for a fault. For the expert it is extremely difficult to get an overview of all possible faults. If the documents provided by the providers do not show any particular inconstancy, the expert will not come to the conclusion that one of the providers committed the fault.

3.6.2.5 *Summary Third Case*

Again, the cloud user will lose the lawsuit against his client, as in this case it is even more difficult to disprove his own fault and a providers fault either, his direct contractual partner or the fault of the person whom the provider uses to perform his duty.

3.7 SLA’s

Within the contract cloud user/cloud provider, the cloud provider has to be contractually bound on how to process the data, what kind of measures he is obliged to use with regard to data protection, and if he is allowed to involve subcontractors. Additionally, it has to be clarified what the modalities of the transfer of the data after the termination of the contract are. Another import point is a possible bankruptcy of the provider. For these cases the cloud contract should foresee ways to permit the user to get his data easily back. A detailed description of the performance and the obligations is mandatory.[82]

So called "Service Levels" are generally concretizing the scope and quality of the service. They are usually separately agreed upon and refer in particular to the performance owed by describing it precisely. Especially the availability of the concrete cloud performance is used as an indication concerning the quality. Other parameters are reaction and fault clearance times in the case of failures or performance and responding times of a specific software.[83]

The European Commission has published a guideline about the drafting of service level agreements which describes the different service level objectives and how to fulfil the requirements.[84] For example, with regard to availability, the level of uptime, the percentage of successful requests and the percentage of timely service provisioning requests should be listed.[85] With regard to response time this shall be divided into average response time and to the maximum response time. Concerning other performance parameters and for a more complete view, we therefore refer on the European Commission's Cloud Service Level Agreement Standardisation Guideline.[86]

3.8 Conclusion for Mirasys Use Case Nr. 1 – Act of vandalism in the night

In this use case, CitySec as the surveillance company has the duty to monitor the metro station which is damaged due to a fault. MetroSub sues CitySec, since the latter didn't fulfil its contractual duty of protecting the metro station from harm. Within this case, CITYSEC has to prove that he did act neither intentionally nor negligently and that also third parties he used to perform the contractual duties did act neither intentionally nor negligently, thus TelCom, TenSys and CloudCorp. CitySec are therefore also responsible for their fault. The current evidence law situation does, however, not permit the cloud user, thus CitySec, real possibilities to contradict the non-default of TelCom, TenSys and CloudCorp. It is thus very difficult for CitySec to win the lawsuit against MetroSub or to successfully take recourse on the providers, TelCom, TenSys and CloudCorp.

3.9 Summary Evidence Law

The current evidence situation of the cloud user is very weak, as without an inside view into internal cloud processing mechanisms, the cloud user can hardly manage to prove the providers fault. This leads to the consequence that the cloud user either loses the lawsuit against the provider directly because he cannot manage to prove a negligent behaviour, or that in cases where he has been sued by his client, he cannot contradict the non-default of the provider and thus disprove an own negligent behaviour by him. The cloud user is therefore reliant on provider-independent proofs, which are neutral and truthful and permit him an inside view into internal

[82] S. D2.2.
[83] Bräutigam, IT-Outsourcing, Part 13, recital 420.
[84] http://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines
[85] Cloud Service Standardisation guideline, p.15f.
[86] Cloud Service Standardisation guideline https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines.

system operations without the assistance of the provider. It will have to be clarified in Section 5 if the technologies developed within the SECCRIT project can be used to strengthen the legal position of the cloud user.

3.10 Data Protection Law – The current legal situation

Within this section we summarize the data protection law problems that have already been delineated in D2.2. We specifically outline and complete the problems occurring in the context of cloud computing. For this we use the Mirasys Use Case 2 - the misbehaving politician - in order to illustrate the data protection problems. Given that the European directive 95/46/EC has been implemented into national law, we will refer to D 2.5 which summarizes the national data protection consultation results, respectively the answers of the Finish and the Spanish Data Protection Authorities.

Since the SECCRIT project is focused on establishing mechanisms that permit to strengthen the legal position of the cloud user, they not only need to be admissible in court, but they also need to be data protection friendly. The core challenge beyond that is to ensure that the technologies cope with the results of evidence law assessment. As evidence law is focused on disclosing facts in order to permit a sustainable legal position in court it is highly challenging to combine it with the data protection regulations, which are more focused on data minimization mechanisms. In this chapter due attention will also be payed to the global challenge of providing the cloud user with a more suitable starting position in court while simultaneously ensuring that no data protection regulations are infringed.

3.10.1 Introduction

Data protection law has the objective of protecting the data subject’s fundamental right for informational self-determination. Therefore, individuals need to be protected against possible infringements of their right caused by handling of their personal data. The underlying intention is that the data subject should have the right to decide to whom his personal data can be disclosed. For this aim, specific legal provisions have to be adhered to whenever personal data is processed. “Processing” is, according to Art. 2b Art. 95/46/EC any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Personal data, in turn, are any data which can be used to identify a specific natural person or can be attributed to such a specific natural person like address, date of birth, phone numbers, email address, bank account number or personnel number.

To a large extent, therefore, the challenges in data protection law stem from the fact that the controller is the one who is responsible for the fulfilment of the data protection law problems as he is the one processing the data. This reason is sufficient enough to provide him with the responsibility to fulfil the data protection regulations. Data Protection law imposes certain duties on anyone who is processing personal data.

It turned out throughout the course of the SECCRIT project that it is necessary to distinguish between two and three party relationships. Within a two party relationship, the cloud user is outsourcing his own personal data into the cloud, whereas in a three party relationship, the cloud user is outsourcing personal data of another person, the so called data subject, into the cloud. Especially the latter case is very relevant in the sector of critical infrastructures very relevant. The operator of a critical infrastructure is the cloud user in that case. In order to understand the data protection problems, we firstly explain the different roles as well as what is regarded as personal data. We focus also on audit trails, as these are very important for the evidence part (see above).

3.10.2 Different roles provided by data protection law

In this section, a fundamental understanding of the different legal roles provided in European data protection law will be outlined. Some important roles – the data subject, the controller and the processor – shall therefore be briefly introduced.

3.10.2.1 *Data subject*

According to Art. 2 lit.a of the European Data Protection Directive 95/46/EC, the data subject is an identified natural person or a natural person who can be identified. An identifiable person is further on one who can be identified directly or indirectly, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Personal data which relates to an identified or identifiable person is processed by another person, the so-called controller. The term processing covers, as stated above, all kind of different operations like collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, see. Art. 2 lit. b 95/46/EC. To sum up, the person, which can be identified by its personal data (processed for a specific purpose by the controller), needs to be protected. For this aim the data subject has some rights like for example, access, information, deletion and blocking rights which he/she can enforce against the controller in order to have a better knowledge about the data processing.

3.10.2.2 *Controller*

As the data subject's personal data have to be protected, this implies that there is, indeed, another person who is processing these data. This person is the so-called controller, who is responsible for fulfilling the data subject's rights like information and access rights. According to Art. 2 lit. d of the European Data Protection Directive 95/46/EC, the controller is "the natural or legal person […] which alone or jointly with others determines the purposes and means of the processing of personal data". Therefore the term "controller" primarily aims to attribute responsibility, as the controller is the person who is ultimately responsible for the data processing.[87]

Consequently, the controller decides about the purpose and the means of data processing. Purpose means the motivation of the data processing, in the sense that the processing has to be carried out because of a specific cause.[88] The means, in contrast, are relating to the technical ways of processing personal data and the question how to achieve it properly.[89] This implies that the controller shall decide about the type of personal data which has to be recorded and

[87] European Commission, amended proposal, 1992, p. 10.

[88] Art. 29 Data Protection Working Party, WP 169, p. 12ff.

[89] Art. 29 Data Protection Working Party, WP 169, p. 13ff.

processed, which processing operations are necessary and which third parties have access rights to the data.[90] If the controller processes data unlawfully, then according to Art. 23 of the European directive 95/46/EC, the person who has suffered damage is entitled to receive compensation from him. Additionally, sanctions could be imposed on the controller in case of an infringement of the provisions, s. Art. 24 95/46/EC.

3.10.2.3 *Processor*

Another role provided by European data protection law is the so-called processor, who is according to Art. 2 lit. e 95/46/EC a "natural or legal person […] which processes personal data on behalf of the controller". "Processing on behalf of the controller" means that the processor and the controller are considered as one unit by data protection law. Therefore, "processing on behalf of the controller" represents a privilege because it enables the "transfer" of personal data to another person without the need of the latter one to have an own legitimation by the data subject. The privileged concept of "processing on behalf of the controller" does, however, only apply within the EU. Whenever personal data are transferred to a non-EU country, the person who is receiving the data requires a further legitimation by law or the data subject's consent.[91]

The privilege of "processing on behalf of the controller" is only possible because it is destined that the controller "controls" the processor and also gives him instructions. The controller making use of this concept therefore has to verify the processor's adherence to these instructions as well as the compliance of technical and organizational measures taken by him – not only before a data processing is effected but also on a regular basis.

The consequence of such a classification is that only the controller has to assure compliance with data protection regulations.[92] In particular, this refers to the above-mentioned rights like informing, deleting, correcting, blocking etc. which have therefore to be fulfilled by the controller alone. This is especially motivated by the intention that the data subject should not be confronted with a mere amount of unknown persons but should rather only refer to the decision-maker, who can fulfil his rights properly.[93]

3.10.2.4 *Application to cloud computing cases*

In order to understand the data protection challenges regarding transparency and thus real controllability in the context of cloud computing, we have to map the above-mentioned roles[94] to those present in typical cloud computing scenarios.

As the classification as a controller is therefore necessary for the determination of the person who – from a legal perspective – has to realize the data subject's rights, it has to be clarified who is the controller within typical constellations of cloud computing. Conceivable possibilities are the cloud user, the cloud provider or both together.

Following the above terminology, it is typically the cloud user alone who determines the purpose of collecting, processing and using personal data. This consequently implies that it is the cloud user who is in the legal role of the controller.[95] The cloud provider, in turn, is to be regarded as

[90] Art. 29 Data Protection Working Party, WP 169, p. 4.
[91] Art. 29 Data Protection Working Party, WP 154, p. 7.
[92] Hustinx, Data Protection and Cloud Computing under EU Law, p. 4ff.
[93] Art. 29 Data Protection Working Party, WP 169, p.10ff.
[94] S. 2.7.2.
[95] Art. 29 Data Protection Working Party, WP 169, p. 10ff.

processor, as he does generally not decide over the purpose of collecting, processing and using the personal data but rather processes data "on behalf of" the cloud user.[96] If he nevertheless processes the data further on for own purposes he is to be regarded as a controller.[97]

Considering the cloud user as controller and the cloud provider as mere processor, however, implies that the cloud user is responsible for any obligations to be complied with. In particular, this also extends to those processes executed at the processor's side as he also has respective control duties.

This being said, we will in the following also distinguish between different concrete constellations (see above) of involved actors.

3.10.3 Personal Data

In this section we now describe the subject matter of data protection law.

3.10.3.1 *General basics*

Data protection law comes into force when personal data are collected processed or used in a certain case. Personal data are, according to Art. 2 lit a 95/46/EC, defined as any information relating to an identified or identifiable natural person (data subject). Within the legal discussion there are two different opinions concerning the question for which person the data subject is identifiable. One opinion is saying that if there is only one single person who can determine the data subject, then these data are personal data (absolute term).[98] The other opinion is asking if the person who is responsible for the processing can identify the person (relative term).[99] The European Court of Justice will currently need to decide about the interpretation of the directive concerning the qualification of IP-addresses as personal data. This decision will be of major importance as it will also decide on the interpretation of the requirements of "identifiable" and thus on which opinion has to be followed. The reference for a preliminary question deals with the question if a provider records the IP address relating to an access of his page, this IP address has to be considered as personal data, because the access provider (and thus another person) has the necessary complementary knowledge for identifying the data subject.[100] A qualification as personal data would lead to the application of the absolute term.

The up-coming data protection regulation apparently favours the absolute term. This is manifested in recital 23: "To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual directly or indirectly."[101] Especially the fact that the wording "any other person" is used, speaks in favour of the absolute term. Further on, Art.4 (1) especially cites the online identifier, which would speak in favour for the classification of IP addresses as personal data[102].

[96] Art. 29 Data Protection Working Party, WP 169, p. 10ff.
[97] Art. 29 Data Protection Working Party, WP 169, p. 11.
[98] *Weichert* in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 3; *Scheja/Haag,* in: Leupold/Glossner (Hrsg.): IT-Recht, Teil 4, Rn. 37 f.
[99] So Gola/Schomerus, BDSG, § 3 Rn. 10; Kazemi/Leopold**,** Datenschutzrecht, § 2, Rn. 39; Härting, ITRB 2009, 35 (36); Dammann in Simitis (Hrsg.), § 3 BDSG, Rn. 24.
[100] BGH, EuGH-Vorlage vom 28.10.2014 – VI ZR 135/13.
[101] Version from 11 June 2015, Council of the European Union, http://www.cr-online.de/Verabschiedete_Fassung_der_Datenschutz-GVO_durch_den_Europaeischen_Rat_v._11.06.2015.pdf
[102] And thus even though "only" the access provider have the necessary knowledge to identify the person.

3.10.3.2 *Application to cloud computing cases*

While the data outsourced within the cloud are to a large extent personal data, it is of more interest if internal processing data can be seen as personal data too. It is therefore highly questionable if audit trails for example can be considered as personal data. The Article 29 Working Group has established an in-depth analysis on the question what can be considered as personal data and came up to the result, that the information which concerns an identified individual thus one that can doubtlessly be distinguished throughout a group of several persons has to be considered as personal data.[103] This means that the information provided corresponds to a particular person independently if this connection is directly or indirectly. Besides the most obvious ones like name, address, phone number, email address also geolocation coordination can be considered as personal data.[104]Audit trails in general can also contain personal data, if they permit to identify the person who actually logged these files, like for example the employee of the acting entity.

An audit trail could for example be used for documenting what happens with the outsourced data but it could also be used within internal management mechanisms. It could log in the first case that the cloud user has modified data within the cloud. This would lead to the fact that within this protocol it is written that the cloud user x has changed data y. Whereas the cloud user x represents personal data, the data itself could also contain a personal data element, like for example, the name of a natural person. In this context, the audit trail could contain two personal data, of possibly two different data subjects. The provider would in that context be the controller, as he would collect the data and process them for own purposes. The audit trails can provide further on information about the time, the type of use beside the real user and any search criteria. Within Section 5 where the tools, which have been developed in the SECCRIT project, will be evaluated. It will be discussed how these audit trails should look like in order to ensure that no rights of the data subject are infringed.

If the audit trails contain personal data, either of an employee or of a client of the tenant, then it is questionable who has to be considered as controller. The characterization as a controller depends on the one who decides about the purpose and means of data processing. In the context of the audit trails of an employee it is however the cloud provider himself who takes the role of the controller, as he is the one who is processing the data of his employee to the cloud user for evidence reasons. He is choosing therefore the purpose (disclosing for evidence reason) and means (technical way). For this data protection procedure he will in particular need a consent or a legal basis of the data subject (his employee), as data will be disclosed to another party (recipient). As it is hardly imaginable that the data subject will give his consent for disclosing personal data of him to the client of his employer, and within employee relationships it is often doubtful if a freely given consent is given due to the dependency,[105] the consent is not a real option for permitting such a transfer. Within the concrete case, the employee must give his consent without compulsion. His interest is a criterion for the voluntary nature. Especially in this context it is highly questionable why an employee should give his consent for enabling the cloud provider to disclose his personal data to the client of that one in order to permit latter one to sue his employer. It is therefore highly doubtful that the consent is freely given.[106] A legal basis could either be the contract of the employer and the employee, but also here the processing is not necessary for the performance of the employment contract. The processing could, however, be

[103] Article 29 Working Group, WP 169, p. 10ff.
[104] See for this Article 29 Working Group, WP 185, p.7f.
[105] Killian/Heussen, Computerrechts-Handbuch, Teil 13, IV. Rn.15.
[106] S. for further details 3.11.1.

necessary for the purpose of the legitimate interest of the controller. This would imply that the controller needs to disclose the personal data to the cloud user. Nonetheless the cloud user does not need to know the name of the employee for evidence reasons it is sufficiently for him to know that they are from the entity of the provider. Therefore the collection of the audit trails should ensure, that no personal data are disclosed to the cloud user, as there is no necessity of disclosing them to him.[107]

3.10.4 Processing on behalf of the Controller

Another important concept in data protection law is the so called processing on behalf of the controller. This concept is structured in the way that the processing of the personal data is carried out by a service provider on behalf of the controller. Within this constellation the controller and the processor are considered as one unit, but it is only the controller who has to fulfil the data subject's rights and it is the controller who is responsible for the fulfilment of the data protection law requirements. Processing on behalf of the controller aims at simplifying processing constellations which are effectuated for another person and therefore on their behalf. It contains consequently a privilege of the legitimation, as the service provider does not need a legitimation of the data subject although he is performing the processing, because he is doing this for the controller. This is the reason why the controller remains fully responsible for compliance with data protection regulations. The relationship between the controller and the processor is subject to a contract which needs to state some important subjects, like duration, what kind of service he needs to provide, what kind of data are processed etc. Additionally the controller has to instruct the processor and the processor can only act in accordance with his instructions. The controller in turn has to control the processor, especially in the beginning of the processing and further on during the runtime of the contract. It is often recognized within legal discussions that the controller does not need to have physical access to the hosting environments in order to fulfil his control rights. Especially in cloud-based scenarios it is sufficient to rely on certifications.[108]

3.10.5 Use of Subcontractors

Within the SECCRIT project, the need of the provider to use subcontractors became evident. Such composed systems, where it is not clear what the provider is doing on his own and which services are provided by others but composed by him, is often used in practice. Such subcontracts are legally permissible, if the controller agrees in writing on the use of subcontractors. The processor can then rely on their provided service and use it to perform the duty he owes to his client. Nevertheless the concept of processing on behalf of the controller is represented also in this constellation with more acting parties. Therefore the requirements set up need also to be respected, when subcontractors are used.[109] The cloud user therefore needs to fulfil his control rights also against the subcontractors. The cloud user should therefore foresee that the contract between the cloud provider and the subcontractor also reflects the contractual terms of the cloud user and the provider's contract.[110] It is recommended that the sub contractual contract contains own control rights for the cloud user against the subcontractor.[111] This means that also in chained relationships, the cloud user is responsible for fulfilling the data subject's

[107] S. 3.11.1.
[108] Thalhofer, Grenzenlos: Compliance beim Cloud Computing, CCZ 2011, 222, 223; Niemann/Hennrich, Kontrollen in den Wolken, CR 10/2010, 686, 691.
[109] s. Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, Section 11, Recital 76.
[110] Art. 29, WP 196, Nr.3.3.2.
[111] Orientierungshilfe Cloud Computing, p.10.

rights and thus the data protection rules must also be met within the sub contractual sphere. It is very welcomed that the draft of the European data protection regulation contains provisions concerning the use of subcontractor. Art. 26 (1a) determines that the processors requires a consent of the controller if he wants to use another processor. Art. 26 (2a) postulates further on that "[…] the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor […] in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."

3.10.6 Type of data in SECCRIT and possible constellations

Last but not least within the SECCRIT project we have to distinguish between the outsourced data and the internal data like for example audit trails which record the ongoing procedures within the system itself. Both types of data can, however, be personal data.[112]

We have therefore identified the following possible constellations:

The cloud user is outsourcing own personal data into the cloud (two person relationship).

The cloud user is outsourcing personal data of the data subject (another person) into the cloud (three person relationship).

Furthermore log files can be considered being personal data as well.

We will now apply those general outcomes on cloud-based scenarios and elucidate the current legal situation.

3.11 Data Protection principles

At this point the data protection principles will be described and an analysis concerning the legal classification of data within SECCRIT will be provided regarding their impact on them.

3.11.1 Legitimacy

The principle of legitimacy requires that any processing of personal data is legally legitimated. In accordance with Art. 7 95/46/EC, this can either be by a consent or a legal obligation. If such a legal basis is missing, the processing is illegitimate.

3.11.1.1 *Outsourced data*

3.11.1.1.1 Constellation 1: Cloud User and Cloud Provider

The first possible constellation is that the cloud user wants to outsource his/her own personal data to the cloud. In this case, the cloud user would not only be the controller but also the data subject.
This is, however, not a legally relevant data protection constellation as there is no other person who is handling these personal data. From a legal perspective, in this context the cloud provider is not seen as another person, as he is fulfilling the role of the processor and is therefore counting

[112] S. section 3.10.2.2.

as one unit together with the controller.[113] Furthermore, the cloud provider can in this case be assumed to have a direct legitimation from the cloud user who is at the same time the subject which the personal data refer to.

However, it is, in case the cloud provider decides to use the personal data for own purposes, imperative for the cloud user and thus the data subject to find out about such conduct. In so doing, the cloud provider would become the controller and would thus be the addressee of the data protection regulation, particularly requiring a legitimation for any such processing.[114] The problem therefore is that the technical property of cloud computing systems (black box nature) does not permit the cloud user to get an inside view in data processing mechanisms. The cloud provider could therefore use the personal data of the cloud user for own purposes without the cloud user having any chance of recognizing such basically illegitimate behaviour. Enforcing rules regarding data protection is thus difficult as long as reliable verification of provider conduct is not possible and only based on "trust".[115] We will elaborate in Section 5 if and how the developed technologies can strengthen the legal position of the cloud user and thus the data subject.

3.11.1.1.2 Constellation 2: Cloud User, Cloud Provider and Data Subject

Within the three person relationship, where the cloud user is outsourcing personal data of another person, the data subject, a legitimation is as well required.

Firstly the cloud user needs a legitimation, either a consent or a legal basis concerning the processing of personal data.

It is questionable if the cloud provider does also need a legitimation. However, as generally a processing on behalf of the controller is given, this constitutes indeed a real privilege in the meaning, that the cloud provider does not need an own legitimation from the data subject, for permitting the processing. This would without any doubt not be practicable as it is difficult to get consents from all data subjects, especially if the controller is outsourcing several data of different data subjects. It is therefore sufficient that the controller has the respective legitimation.

3.11.1.2 *Internal management data*

Concerning the log files, as already stated, it is quite difficult to find a real legitimation basis, as a consent will probably not be considered as freely given. Any other particular legal basis of the catalogue of Art. 7 95/46/EC does neither seem to be applicable: the employment contract cannot be the legal basis for disclosing personal data to the contractual partner of the employer, Art. 7, lit. b 95/46/EC. Legal obligations in terms of Art. 7, lit. c 95/46/EC are those ones regulated by national rules or at Community level.[116] Such a regulation which forces controllers to disclose personal data of his employee to the cloud user is up to now not foreseen. Even the upcoming data protection regulation, which will be valid in all countries at once the day it comes into force and would regulate fully all data protection procedures does as well not foresee such a legal legitimation. Protecting the vital interest (lit. d) as well as performing a task carried out in the public interest (lit. e) is not fulfilled by disclosing data of the employee. Finally according to Art.7f 95/46/EC the processing is allowed for the legitimate interest of the controller, third party or parties to whom the data are disclosed. It is, indeed, in the interest of the cloud user to have such audit trails in order to have a better position in court. However Art. 7f 95/46/EC foresees a

[113] Art. 29 Data Protection Working Party, WP 169, p.10ff.
[114] Art. 29 Data Protection Working Party, WP 169, p.10ff.
[115] International Working Group on Data Protection, p. 3.
[116] EC Nr. C311. 27.11.1992, p.17; Ehmann/Helfrich, EG-Datenschutzrichtlinie, Art. 7, section 22.

weighing of respective interests.[117] Whereas on the one side, the data subject has fundamental interests of a non-disclosing, on the other side the interest of the cloud user of getting such personal data is not obvious. The cloud user is only interested in the content of the data, but not on who of the provider's employees committed a possible fault. It is indeed sufficient for the cloud user to know that a fault has been committed in the realm of the cloud provider, respectively someone acted negligently. Therefore, there is no necessity (see also necessity principle 3.11.3) for the cloud provider to disclose this particular personal data to the user.

3.11.2 Purpose-Boundedness

The principle of purpose boundedness states that the personal data have to be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes. A change of the purpose would require a new legitimation.

3.11.2.1 *Outsourced data*

3.11.2.1.1 Constellation 1: Cloud User and Cloud Provider

Concerning the two person relationship the same applies as stated in 3.11.1.1.1. If the cloud provider starts to use the data for own purposes, he would become the controller and the data subject, thus the cloud user can assert his rights against the provider. It is therefore important to enable the cloud user to find out about such conduct.

3.11.2.1.2 Constellation 2: Cloud User, Cloud Provider and Data Subject

With regard to the three person relationship, this principle is not infringed as the data in the cloud are recorded in the realm of the provider for a specific purpose which has been determined between the data subject and the controller. The fact that the data are outsourced further on in the realm of the provider does not present any significant change to the purpose set out together with the data subject, as the data are still processed for that scope. The difference lies in the fact that the data are not saved on an internal server but on servers of someone else who is however considered as the extended arm of the controller. Therefore the purpose of the original scope is still given, when data are outsourced on external servers.

If the cloud provider would start to use the data for own purposes, then he would within this constellation be the controller and he would himself need a legitimation either by consent from the data subject or on a legal basis.

3.11.2.2 *Internal Management Data*

The collection of audit trails concerning the internal management procedures, like for example collecting data about who has updated the software is necessary for the security and maintenance of the system itself. The cloud provider has a legitimate purpose for this as he wants to know that the functionality of the system is ensured by his employees. For this collection he will need a legitimation, like a consent of his employee or a legal basis. The legitimate interest could indeed be estimated as higher weighing as the fundamental right of the employee, as it is in the

[117] Damman/Simitis, EG-Datenschutzrichtlinie, Art. 7, section 12.

interest of the cloud provider to know what his employees are doing, especially for security reasons.

However, the fact that the personal data of the employee are disclosed to the cloud user, will cause a change of purpose, as the cloud provider would then process the data for another purpose, namely for evidence gathering. This change of purpose requires a new legitimation, which, as already seen, is not legally anchored. Therefore the provider needs to ensure that no personal data are disclosed to the cloud user.

3.11.3 Necessity/Proportionality

The necessity principle ensures that personal data are only collected if it is necessary for attaining the specific purpose. Especially when the purpose does not require the collection, processing and using of personal data, such a processing is not legitimate.

3.11.3.1 *Outsourced data*

3.11.3.1.1 Constellation 1: Cloud User and Cloud Provider

Again within the two personal relationship no specific infringement is given.

3.11.3.1.2 Constellation 2: Cloud User, Cloud Provider and Data Subject

Concerning the outsourced data, the same applies as already delineated in the purpose-boundedness section. If the collection, processing and using of the data is required for attaining a specific purpose, this is still the case, if cloud-based solutions are used.

3.11.3.2 *Internal Management data*

As the collection, processing and using of the data of the employee for own purposes of the cloud provider can be considered as necessary, this is not the case for the transfer of the data to the cloud user. The cloud user does only need the content of the data, respectively what has been done. It is sufficient for him to know that within the realm of the provider a negligent or non-negligent behaviour happened. He does not need the concrete name of the acting employee of the cloud provider for sustaining his claim.

3.11.4 Data Minimization

The principle of data minimization aims at limiting the processing of data to the smallest possible extent in order to prevent an encroachment of fundamental rights. Especially anonymization and pseudonymization techniques are valuable possibilities to fulfil this principle. Anonymization mechanisms are of strong interest in the context of cloud computing as in the case of anonymization the data protection regulations are no more applicable.[118] This is however not the

[118] S. Roßnagel/Scholz, Datenschutz durch Anonymität und Pseudonymität: Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2001, 721, 726; Gola/Schomerus, section 3 Note 14.1, 14.2; Tinnefeld/ Ehmann, p. 187; Kilian/Heussen-Weichert, CompHdB, chapter 132, recital 147.

case for pseudonymization techniques as there still remains a person who is able to make an attribution of the pseudonym to the respective person. For now, Art. 30 of the draft of the European Council stipulates in Section 1 that “the controller and the processor shall implement appropriate technical and organizational measures, such as (…) pseudonymisation of personal data to ensure a level of security. If the upcoming data protection regulation opts in favour of the absolute term, it is indeed questionable what the use of pseudonymization would be, as these data would still be considered as personal data. Especially the distinction between non-personal data or data which are pseudonymized and still personal data will be difficult to provide. This would lead to the undesirable consequence, that even though the person is not recognizable, the controller would need a legitimation, due to the specific characteristic as personal data. A consent would in this particular context not be possible, as the controller cannot identify himself the data subject. It is therefore preferable that the data protection regulation contains privileged rules for the pseudonymization as without it the significance of such mechanisms will become obsolete.

3.11.4.1 *Outsourced data*

3.11.4.1.1 Constellation 1: Cloud User and Cloud Provider

Again; the data protection relevance is not given. However it might be important for the cloud user that the cloud provider cannot assess the content of the data. Therefore anonymization and pseudonymization techniques are useful to ensure that the provider does not have knowledge about the content of the outsourced data.

3.11.4.1.2 Constellation 2: Cloud User, Cloud Provider and Data Subject

Concerning the three person relationship it is indeed preferable that the personal data are anonymized before they are outsourced in the cloud in order to prevent the provider from using them for own purposes. If, however, they need to be processed further on, such anonymization techniques do not seem to be useful, as they would still need to be modified and therefore the personal data are possibly needed in a non-anonymized way.

At least for evidence reasons it is necessary to have a possible comparison between the outsourced data and modified data which could possibly represent a damage. Therefore anonymization mechanisms are in the light of the evidence situation not practicable, if the personal data component is necessary for liability reasons. This is mainly due to the fact that there still needs to be a way to use the data as proofs in court in order to demonstrate a possible fault.

Outsourced data could therefore as well be useful for evidence reasons. If for example the data are modified this can cause a real damage for the cloud user, as he would no longer have his originally outsourced data or at least the content of them in the way he wanted to outsource them. Especially if this modification has been caused by the cloud provider, the cloud user might want to assert a claim against his contractual partner in order to get his damage back. For this he is required to have some proofs, which must simultaneously be data protection friendly.

Pseudonymization techniques are an interesting option concerning the outsourced data, in order to prevent the provider to have an inside view in what the user is outsourcing.

Since the cloud provider is generally seen as a processor at least pseudonymization mechanisms would prohibit that the provider sees the content of the data, as he cannot easily reattribute it to a natural person. He does, as a processor, not need to have a particular legitimation as seen above. Therefore from a legal theoretical reason such mechanisms are not necessary, as it is only the controller who is the addressee of the fulfilment of the data subject's rights. For practical reasons and especially because control mechanisms are missing it is however preferable to ensure, that the provider does not have insights in the content of the outsourced data.

The data do not need to be fully perceivable by the cloud provider for fulfilling his duty of providing a functioning system. However, if the provider changes the data and this leads to a damage for the cloud user, the originally outsourced data need to be used as a proof in court as well as the changed data. If the cloud user has outsourced pseudonymized data, these "original" data need to be shown in court as proofs. The modified data need further on to be shown as well. The comparison between original and modified will then show the possible fault. It will afterwards be questionable if the modification of the data has been caused by the cloud provider negligently. Therefore data protection problems will mostly occur if the cloud user outsources personal data from the very beginning. As it is, however. very likely that the absolute term is applicable, even pseudonymized data would be counting as personal data, therefore data protection regulations will still remain applicable. Disclosing the data for evidence reason to the party which requires proofs could infringe data protection regulations. However, as seen in the evidence law part it is the cloud user which legal position is weak, therefore he is the one who is in need of getting neutral proofs. Proving that original outsourced data have been modified by the cloud provider will however not be as difficult as proving a negligent behaviour concerning internal management system operations. Especially in the latter case, the user misses an inside view in such processing's. What still would be necessary for proving that it was the provider who modified the outsourced data would indeed be a log file which documents such a proceeding. If data are pseudonymized and later on changed the user still needs to attribute this modification to the provider. Such data are internal management data.

Further on, it is questionable if the disclosing of personal data in court is legally admissible and thus which specific legal basis is given. Art. 7f 95/46/EC could be applicable as it is the legitimate interest which would weigh higher in comparison to the fundamental interest of the data subject. In accordance with the proportionality principle and depending on the circumstances of the individual case the interest of a sustainable legal case in court will mostly be weighed higher.

To sum up, anonymizing personal data will only be practicable as far as the personal data in their non-anonymized version are not necessary. For evidence reason and depending on the way data have been outsourced in the beginning such techniques might not be useful if the anonymization has been conducted after the outsourcing.

Pseudonymized data could be used as evidence in court, if they have been outsourced in this way. As they would still contain personal data, this would constitute the fact, that the user has a legitimation for such a transfer to the court. This transfer, can depending on the individual cases be legitimated by Art.7f 95/46/EC. Still the outsourced data will not be sufficient alone for sustaining the case of the cloud user. The cloud user will also need internal management data for proving that it was the provider who committed such a modification. In section 5 it will be outlined, if such a proceeding is technically feasible.

At least the comparison between outsourced data and modified data needs to be done in order to see if a fault is given. If therefore the outsourced data have already been pseudonymized or anonymized before the outsourcing, then the cloud provider owes to maintain them in their original outsourced version. If data are modified in an unauthorized way it will have to be determined within the court, whether there is a change between outsourced and modified data. Pseudonymization and anonymization techniques are thus mainly useful before data are outsourced in the cloud.

3.11.4.2 *Internal management data*

Keeping the necessity of a reattribution for evidence purposes in mind it is of high interest that not only the provider has access to the audit trails but also the user in order to have equal starting positions in court. Regarding audit trails, again anonymization techniques are therefore not useful, as those data need to be uncoded as they are required for the evidence part in order to demonstrate what respectively has been done. This is why at least an anonymization will not work, as afterwards there is no other person who would be able to decrypt the data, facing the problem, that it cannot be used as evidence. Pseudonymization would be a possible way to limit the risk of an encroachment on the data subject’s fundamental rights. It still remains questionable who will be in charge for the pseudonymization. This could be the provider, the user or a Trusted Third Party for example. Several solutions could be conceivable:

- The audit trails are recorded in the sphere of a trusted third party. This Trusted Third Party has a system map of the original one from the provider. In case of a lawsuit the trusted third party acts as a witness, especially concerning the storage system. The expert can then analyse the data and make his report.
- The audit trails are additionally directly sent to the cloud user. In so doing the cloud user has directly the proofs.
- The audit trails are recorded in the sphere of the provider. Only the Trusted Third Party has the key to unlock the files.

However all these solutions would require the necessity of transferring personal data to the cloud user or the Trusted Third Party. As within the first solution pseudonymization mechanisms might be useful in order to ensure that the Trusted Third Party cannot access the data, we clarified that the cloud user only needs to know the content. This audit trail therefore does not need to contain personal data. The transferred data to the Trusted Third Party therefore do as well not need to contain personal data. This means that the internal management data which might be disclosed by the Trusted Third party or in the second case by the cloud user do not represent personal data and therefore data protection provisions do not apply in this context. Anonymization and pseudonymization techniques for data protection reasons do therefore not need to be conducted.

3.11.5 Transparency

For achieving the data subject’s informational self-determination, the principle of transparency is highly significant. Following this principle, it has to be apparent for the data subject, by whom and for what purpose the processing of personal data takes place. Transparency is ensured by information and access rights as stated, for example, in Art. 10, 11, 12 of the European data protection directive 95/46/EC. Only with knowledge about a processing of his/her data, the data subject can recognize an infringement of his fundamentally protected informational self-determination and can then exercise his/her rights. In particular, the data subject can assert to rectify, erase and block data which has been collected concerning him or her. A breach of data protection provisions, like the non-performance of such stated data subject’s rights, leads to civil/criminal proceedings.

To a large extent, the use of cloud computing is currently based on users trusting in the providers’ reasonable conduct in handling their data. Negative headlines and increased awareness throughout the business as well as the consumer domain call however for more authoritative mechanisms, especially permitting the cloud user to achieve real control over his/her outsourced data.

The intentional opacity of cloud computing systems, however, stands in diametrical contrast to this aim: At least currently, it is one of the core concepts of cloud computing that the cloud user does not have an inside view of the cloud system itself and can therefore not assess what actually happens with his/her data. From a legal point of view this is highly critical, as especially data protection law requires a transparent[119] handling of personal data, implying that the data subject needs to be aware of what happens with his personal data. This is already challenging for cases where the cloud user himself is the data subject and wants to use cloud computing systems as he will not know what the cloud provider is actually doing with his/her data. All the more, fulfilling the need for transparency is challenging for situations where the cloud user himself/herself is not the data subject but rather wants to process personal data referring to a third party (the data subject) within a cloud-based service – as it is, for instance, the case for cloud-based customer-relationship management systems etc. Finally, in case the cloud provider on his part again resorts to other cloud providers (e.g. for basic block storage or a hosted database) and thus offers a composed cloud system to the user, the legal requirements for transparency can hardly be met in practice.

3.11.5.1 *Outsourced data*

3.11.5.1.1 Constellation 1: Cloud User and Cloud Provider

Within the first constellation the intended opacity and thus a lack of transparency could lead to the undesirable constellation where the cloud provider uses the personal data for own purposes, which would be a violation of data protection law, but where such an infringement of law cannot be recognized as no reliable verifications of provider conduct are provided. Even though the cloud provider would be in these cases the controller and the data subject, thus the cloud user could assert his rights against the provider, the lack of knowledge of the user about such conduct will prevent him from taking legal measures.

Additionally, also contractually bounding the cloud provider to disclose actual details of data handling, including the location of the data as well as other relevant information, will as well not be sufficient as the cloud user could again not verify the true compliance with such a contractual clause. The currently predominant practice of trusting the cloud provider should therefore be transformed into a real control option, permitting the cloud user to recognize an infringement. This means that it might be valuable to think about technical mechanisms which can help the cloud user find out what actually happened within the cloud-based system. In so doing the cloud user could see that his data are used for own purposes and could then assert his rights directly against the provider.

3.11.5.1.2 Constellation 2: Cloud User, Cloud Provider and Data Subject

In cases where the cloud user outsources personal data of a third party, ensuring transparency for the data subject becomes even more challenging. The cloud user would in these cases be the controller, and it will thus be him who would have to fulfil the data subject's rights, e.g. access, information, correction, deletion or blocking etc. The cloud provider, in turn, would generally be

[119] Transparency in the common meaning of disclosure, as opposed to the technical term opacity.

classified as a processor with the questionable consequence that, even though the personal data are in his/her sphere, he/she is not the one who has to fulfil the data subject's rights. This might from the data subject's view be reasonable, as the data subject will not know the cloud provider, and the data subject should not be confronted with unknown persons.[120]

The problem however is that the cloud user can hardly fulfil the data subject's rights properly if he/she is not in the position to reliably assess the actual conduct of the cloud provider. The actual system design does not provide the cloud user with an inside view in operational processing details. The cloud user can thus not know what actually happens with the data that he/she outsourced into the sphere of the cloud provider. This is all the more intensified in cases where cloud providers are using sub-contracts. Their respective processes and procedures are in this context not disclosed, leading to the legally unsecure situation that it is increasingly invisible to the cloud user what happens with the data of the data subject. Moreover, within composed cloud systems and depending on the concrete technical design, it is even difficult for the cloud providers themselves to deduce where the data are hosted in real-time, especially on which physical machine, data centre or global region.[121] As a result, information rights of the data subject are hardly realizable.

Further on, if the data subject exercises his right of erasing his data, it is not guaranteed that this is truly executed within the sphere of the provider or his subcontractors.[122] This leads to the undesirable situation that the data subject's possibilities to critically review the handling of his data are significantly restricted. Fulfilling the rights of the data subject properly therefore requires that the cloud user gets an inside view into the data processing and can really determine whether the data subject's exercised rights are executed properly.

Therefore, it is mandatory that the use of cloud computing still enables individuals to be clearly informed in a transparent way about how and by whom their data are collected and processed, for what reasons and for how much time they will be recorded and that the execution of exercised rights is properly ensured.

The concept of processing on behalf of the controller is presenting a real privilege in the meaning that the "transfer" of the data into the sphere of the provider is not counting as one which requires the fulfilment of the provisions and principle of data protection being met by the processor himself, as he is only the extended arm of the controller. This is intended by law, because the controller has to instruct and control the processor and the processor is limited in processing the data only for the purposes set up by the controller. The contract between the controller and the processor is forming the legal basis for this. However again the lack of possible verification of the compliance of the provider with set up duties makes the application of the concept of "processing on behalf of the controller" for cloud computing cases very inappropriate.

Additionally it is also difficult for the cloud user to fulfil his duty of controlling the provider. He has very restricted possibilities to acquire provider-independent information about the technical and organizational measures employed by the provider or to even get physical access to the hosting environment in order to fulfil his/her legal control obligations. This control duty and thus establishing transparency is within the legal discussions often solved by the recommendation of relying on a provider whose services have been certified.[123] However the fact that a certification is given does not release the controller from his control duty.[124] The certification does not indicate

[120] Art. 29 Data Protection Working Party, WP 169, p.4ff

[121] EuroPriSe, European Privacy Seal. Cloud Computing and European Data Protection Law; Art. Data Protection Working Party, WP 196, p.13.

[122] Pearson, p. 4ff.

[123] Bergmann/Möhrle/Herb, § 11, Rn. 48b; Art.-29-Datenschutzgruppe, WP 196, p. 22; Weichert, DuD 2010, 679, 683; Heidrich/Wegener, MMR 2010, 803, 806; Hornung/Sädtler, CR 2012, 638, 643.

[124] Orientierungshilfe Cloud Computing, p. 10.

that data protection provisions are met, but only that a security concept is given. The certification according to ISO 27001 is not meaningful for data protection law.[125] Additionally the certification is only confirming the status relating to the time the certification has been given. It does not guarantee that this is still the case when the outsourcing is executed. Consequently this should require a new certificate. Further on the certificate is only attributed in general and therefore for all the users simultaneously. The user cannot have a guarantee that the specific service he requires underlies the certification procedure.

Fulfilling the rights of the data subject as a consequence of the transparency principle can thus not be achieved by certifications. These cannot permit the cloud user to really assess where the data of the data subject are, if data have been modified/erased etc. Even though the processing on behalf of the controller contains privilege in the meaning that the processor is not a recipient, as he is according to Art. 2 (f) 95/46/EC not a third party, it is attributing the responsibility of fulfilling the rights of the data subject to the cloud user. Therefore he needs to have the knowledge about the handling of outsourced data in order to fulfil the rights of the data subject truthfully and correctly. Otherwise he is risking sanctions and legal proceedings.

The cloud user thus could fulfil them, if he would have technical mechanisms permitting him/her to directly realize the data subject’s rights and to control the cloud provider. As the legal consequence of a violation of data protection provisions can lead to civil/criminal proceedings, the cloud user requires possibilities to directly fulfil those rights. Insofar, the outsourcing of personal data to the cloud is from a legal point of view highly questionable as for now the cloud user can only delegate the fulfilment of those rights to the cloud provider, without being able to verify the true value of it, risking legal proceedings. Therefore, neutral technical mechanisms permitting transparency (as opposed to the opaque cloud system design predominant today) and permitting true control are legally indispensable. These mechanisms would go far beyond the possibilities that a certification provides and can thus permit even in cloud computing settings the fulfilment of the transparency principle. In chapter 5 we will outline if the technologies developed within SECCRIT do help to strengthen the legal position of the cloud user.

It is further on very welcomed[126] that within the draft of the European Council from 11.06.2015 in Art. 26 (2(e)) it is stated that the processor shall “assist the controller in responding to requests for exercising the data subject’s rights laid down in chapter III”. Additionally Art. 26 (2(h)) stipulates that the processor shall “make available to the controller all information necessary to demonstrate compliance with the obligations […] and allow for and contribute to audits conducted by the controller”. Therefore implementing such technical solutions would be conforming to the provisions in the draft, as they would permit the assistance of the processor[127]. By this the cloud provider could adequately fulfil the duty of making the necessary information available to the controller. Therefore the cloud provider has a direct legal duty to assist the controller. At least this could be a motivation to implement such technologies as he could show that he acts in conformity with the legal requirements. In order to prohibit legal proceedings, neutral technical mechanisms are therefore highly precious and will permit real possibilities to truthfully assert the rights of the data subject.

[125] Orientierungshilfe Cloud Computing, p. 10.
[126] At least if those provisions are maintained in the final version of the data protection regulation.
[127] “make available, contribute”, as stated in Art. 26 (2h).

3.11.5.2 *Internal Management*

As the internal management data should not contain any personal data, at least the cloud user as the controller is not legally bound to fulfil the transparency principle. Otherwise he would have been obliged to inform his employee about the processing. In return the employee can assert his rights that the provider has to fulfil.

3.11.6 Data Security

The principle of data security states that the controller has to implement appropriate technical and organizational measures for the protection of personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. The technical and organizational measures have to guarantee a level of security which is appropriate to the risks related to the processing of personal data.

3.11.6.1 *Outsourced data*

3.11.6.1.1 Constellation 1: Cloud User and Cloud Provider

As the first case does not present any direct data protection problems, we will concentrate on the three person relationship.

3.11.6.1.2 Constellation 2: Cloud User, Cloud provider and data subject

As we generally have a processing on behalf of the controller, Art. 17 95/46/EC states that “*the controller has to choose a processor providing sufficient guarantees in respect of the technical securities measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures*”. Especially the latter sentence implies a control right of the controller. With the up-coming data protection regulation new wordings have been chosen:

The former draft of the European Commission from 25.01.2012 COM(2012) 11 final uses the following wording in Art. 26 (1)[128]:
“[…] the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation […] and shall ensure compliance with those measures”.
The draft of the European Parliament from 12 March 2014[129] adopts the same wording as the draft of the European Commission.
The draft of the Council of the European Union from 30.06.2014 11028/14[130] states the following:
“The Controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures […] in such a way that the processing will meet the requirements of this Regulation.” This sentence contains a reference where it is stated that “the latter part of the sentence was deleted as it added nothing substantial”. Without the wording of ensuring compliance with those measures it is highly questionable if the control duty of

[128] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[129] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN
[130] http://www.cr-online.de/ST_11028_2014_INIT_EN.pdf

the controller is still foreseen. However the indication that “it added nothing substantial” specifies that the control obligation is still immanent. For reasons of clarification the half sentence should however be maintained as the interpretation of the wording alone will make it difficult to retrace the meaning of the legislator.

The draft of the Council of the European Union from 11.06.2015 9565/15[131] finally stipulates the same wording as in the draft of 30.06.2014. Art. 26 (2aa) is stating further on that the “adherence of the processor to an approved code of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate sufficient guarantees […]. Such a certification would be helpful to demonstrate that a neutral organization has audited the services along recognized standards and has determined adherence with the specific requirements. However such certification should be made continuously in order to ensure the adherence of appropriate technical and organizational measures constantly. Especially Art. 39 (4) which foresees that “ the certification shall be issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions as long as the requirements continue to be met”, does not seem to be appropriate for cloud computing cases. Depending on the specific (special) categories of data, certifications should be at least continuously in a shorter amount of time carried out in order to ensure that requirements are continuously checked. Certifications are therefore a good option to turn the trust of the cloud user in an independent and truthful audit.

3.11.6.1 *Internal Management*

Again, as the internal management data should not contain any personal data, questions about data security in the context of data protection law do not rise up.

3.12 Conclusion for Mirasys Use Case Nr. 2

In the Mirasys Use Case Nr.2 – the misbehaving politician, CITYSEC as the security company outsources the operation of a video surveillance system and determines the purpose and the means of the processing. CITYSEC is therefore the controller. The politician is thus the data subject as he is the one who is being recorded on video within the metro station. His identity can be determined by the video camera images. Therefore he is the one who needs to be protected against a possible infringement of his informational self-determination right caused by a handling of his personal data. As a result, CITYSEC has the responsibility to fulfil the data subject’s rights.

The use case primarily deals with questions of data leakage. Within this case processing and storage of video images are outsourced into the cloud. Such images do also represent personal data, s. recital 14 95/46/EC. Excluding the fact that the picture of the vomiting politician also implies liability questions, it exemplifies the lack of transparency within the cloud. Since no logs are available it cannot be retraced who copied the pictures. This simultaneously also shows that someone used the data for own purposes and that the cloud user has/could not recognize such an infringement. The cloud provider or even anyone else can use the data without a legitimation and the cloud user as the controller will even not recognize such an infringement. The current legal situation does not permit an inside view in ongoing processes.

Even if the cloud provider has received a certificate this is not a sufficient indication that no faults leading to data breaches can occur. Thus certification cannot protect from attacks or

[131] http://www.cr-online.de/Verabschiedete_Fassung_der_Datenschutz-GVO_durch_den_Europaeischen_Rat_v._11.06.2015.pdf

misconfigurations. In turn technical mechanisms could be highly valuable to prevent on the one hand faults and on the other to repressively assess what has happened. Especially if the cloud provider has followed the instructions of the cloud user and a fault still occurred the controller remains the responsible party at least concerning the external relationship. Only if the controller can prove that he has made all the necessary efforts and the processor still has exceeded the instructions he can be relieved from responsibility. This case illustrates therefore that the current legal situation does not permit the cloud user to really assess the processes in the cloud, therefore technical monitoring mechanisms could be helpful.

3.13 Summary

The current legal data protection situation shows that cloud computing cases cannot be easily subsumed under the existing legal framework. At least the obligations underlying the concept of processing on behalf of the controller, which is seen as a privilege, can hardly be fulfilled without the involvement of the cloud provider. Especially the lack of transparency does not permit the cloud user to really assess the handling of the data by the provider. Based on a rigorous application of principle-related obligations from data protection law to typical cases of cloud computing, a major lack of transparency and thus real “control” options for the cloud user were identified: When personal data referring to a data subject are outsourced to cloud systems, transparency gets lost as current practices of cloud computing do not provide the cloud user with the inside view into operational processing details necessary to assess what actually happens with this data. Such an inside view is, however, mandatory for achieving compliance with the principle of transparency from data protection law in the context of cloud computing. Even more than in usual settings of cloud computing, this is the case for composed cloud systems where cloud providers are using sub-contracts. Within such settings, it is even more opaque to the data subject what happens with his/her data. Fulfilling the transparency principle therefore calls besides the use of certification which is important for independently checking if appropriate organizational and technical measures are met, for novel options allowing to truly execute data subjects’ transparency-related rights. For now, the capabilities of existing technical mechanisms in this regard are strongly limited, leading to the legally critical situation that transparency rights can only insufficiently be implemented in the context of cloud computing. Novel, provider-independent technical mechanisms supplying the cloud user with an inside view into data handling processes and at the same time ensuring a significantly higher trustworthiness than provider-maintained frameworks are therefore indispensable.

4 Recommendations concerning liability/evidence law and data protection law

We identified that the current legal situation with regard to liability/evidence law and data protection law shows a massive lack of transparency. This leads on the one side to a weak legal starting position in court with major difficulties of the cloud user to substantiate its case and on the other side to fulfil the data subject’s rights properly. The cloud user has thus no real control options and has no inside view on processing within the cloud, which could help him to assess possible infringements. As a result we are therefore opting for technical mechanisms that can ensure the rights of the cloud user and thus the data subject more effectively.

Another possibility would be to adapt the legal framework in such a way that the position is strengthened directly by law.

4.1 Adapting the legal Framework

4.1.1 Liability/Evidence

Liability and evidence law are determined processes that will hardly be changeable. There is always going to be a party which has to prove facts and the adversary party has to disprove it. A reversal of the burden of proof is also not useful in cloud computing cases as the proofs still remain in the realm of the provider. The provider is always in a better proving position because he is the one who is managing the "content" of the audit trails. It is therefore very difficult to really assess what is actually going on within cloud based systems.

4.1.2 Data Protection Law

The fact that European data protection law is undergoing a major change calls for action, especially because the directive will be replaced by a regulation which will be valid in all countries from the day it comes into force without the necessity to implement it into national law and no adoption has yet been realized. A possibility would be to make the cloud provider the direct responsible party. This would, however, lead to a major change concerning the systematic of data protection law, which does only attribute the responsibility to the controller. This is appropriate as he is the one who is deciding about the means and the purpose of the processing. Consequently he has to be the one who is fulfilling the data subject's rights. The provider is only in very few cases conducting the processing for own purposes. Therefore, the fact that the data are in the realm of the provider is not sufficient enough to provide him with the responsibility intended by data protection law. Heightening the transparency by forcing the provider to assist the cloud user like it is planned in the draft of the European council is a promising way and should be maintained. However intensifying the possibility to audit the handling of data within the cloud, needs also to be taken into account. As audits are basically easier feasible by technical means, it is necessary to legally ensure that the provider supplies technical mechanisms that could permit a direct inside view in on going internal processes.[132]

4.2 Technical ways of strengthening the legal position of the cloud user

Besides adapting the legal framework we propose to strengthen the legal position by technical mechanisms. Given the current lack of transparency, we will now identify what requirements need to be fulfilled by the technical mechanism aimed at closing the identified gap.

4.2.1 Objective of Technical Mechanisms

As outlined above, most data protection rights (including those related to transparency) need to be fulfilled only by the cloud user because the cloud user and the provider are generally, legally counting as one unit in case of "processing on behalf of the controller". Thus, the cloud user needs to be able to discover any collection or processing of the personal data carried out by the provider for own purposes, as this would imply that the provider becomes a controller. Therefore he/she requires an inside view on what the provider is doing with the personal data.

Moreover, if the data subject wants to delete his/her data, the technical mechanism should permit the cloud user (who is responsible for ensuring the data subject's right's to be complied with) to

[132] See for this chapter 6.

determine whether the personal data are effectively erased on all servers, even including the meta-data in order to ensure that no attribution to the specific natural person is possible anymore.[133]

Furthermore, as the composition of cloud services from other ones without this composition being visible to the cloud user is characteristic for cloud computing, the cloud user does not have the possibility to detect a possible data transfer to locations that do not have an appropriate and recognized level of data protection. This therefore implies that technical mechanisms should enable the cloud user to know the actual location of the data in real time in order to be able to react if data are transferred to non-European countries. Again, this calls for technical mechanisms providing an inside view and allowing detecting such data transfers.

Finally, it is also preferable to provide technical mechanisms which permit to control continuously that the cloud provider employs sufficient technical and organizational measures in matters of security. This requires that procedures and practices regarding the chosen security mechanisms are technically disclosed.

Altogether, the cloud user thus needs technical mechanisms which enable him to get a reliable inside view on what the provider is doing with the personal data of the data subject. This includes the location of the data as well as other relevant information as mentioned above. Without such an inside view, the cloud provider can hardly fulfil his transparency obligations from data protection law.

4.2.2 Technical Design

Given these requirements, technical mechanisms for providing adequate transparency in the context of cloud computing must go well beyond the state of the art of monitoring tools in order to prohibit that cloud providers tamper outputs of used technologies. The cloud user therefore needs an independent view onto the lower layers of the cloud infrastructure thus the physical components in order to pursue the above-mentioned objectives.

Such technical mechanisms which could provide the required information would as well also needed to be secured in a way that they are themselves not able to be tampered by the provider and thus produce at any time a system view that represents the reality.

Since these technologies will have to play an important role in achieving compliance with the identified requirements from data protection law, the technical design of such systems should especially permit the cloud user to extract the following information:

Erasure: As mechanisms allowing detecting a requested data deletion on all possible instances are necessary, the technologies should enable to retrace all possible copies to ensure that all data is deleted.

Location of data: The technologies should be able to detect the location of data especially if data stay in the European Union or are transferred to non-European countries. This means that the technologies should recognize the exact physical location of the infrastructure system and deduct from used virtual machines the physical component and thus the exact geographical location to which it belongs to.

Used security measures: Technologies should be able to reflect the used security measures and provide information about applied updates etc.

[133] Art. 29 Data Protection Working Party, WP 154, p.4ff.

Access of data: Technologies should further on be able to monitor accesses on the outsourced data, like using data for own purposes.

Business Secrets: The information gathering must also support mechanisms which do not reveal business internals of the provider.

Last but not least besides gathering information, it must be ensured that the information is stored in a tamper-proof and non-repudiable way. Thus; involving trusted third parties should be anticipated in order to ensure the credibility of such data. Otherwise the trustworthiness of such information remaining in the realm of the cloud provider could still be highly doubtful.

Within the next chapter we will check, if the tools which the technical partners have developed are proving to be highly valuable for strengthening the legal position of the cloud user and thus the data subject.

5 Legal Evaluation of Technical Tools

Within this section we evaluate all RTD outputs. We will firstly describe briefly the scope and the function of the system by particularly paying attention to a possible record of information of the system itself and afterwards assess all tools from a legal point of view. The legal analysis is provided both with regard to liability and evidence law as well as in the light of data protection law. The legal assessment is completed by an application on the Mirasys Use Cases 1 and 2 by showing if the developed tools might be helpful for solving the cases and addressing the currently given problems stemming from the field of evidence and data protection law with their specific impact on cloud computing scenarios. A summary of each tool is provided at the end of every legal assessment.

5.1 How the legal findings have influenced the technical work

Before assessing the technical tools from a legal point of view we want to show our guidance work within SECCRIT. Besides adding in each technical chapter a section with legal questions, which the technical partners had to fill out, we concentrated on the system design of the technologies. We did not only focus on ensuring that the technologies themselves are legally conform, but that they also permit to heighten the legal position. After establishing the use cases in a way that they also are useful in a legal manner, we also finally set up two test cases 008 (Geolocation of sensitive data) and 009 (legal evidence provision) to show how the technologies can be used to strengthen the legal position. We therefore test the developed technologies for their legal usefulness.

All technical deliverables are therefore somehow linked to the legal output:

Fig. 3 describes the link included with the demo cases, whereas in Fig. 4 the output clusters are directly shown.

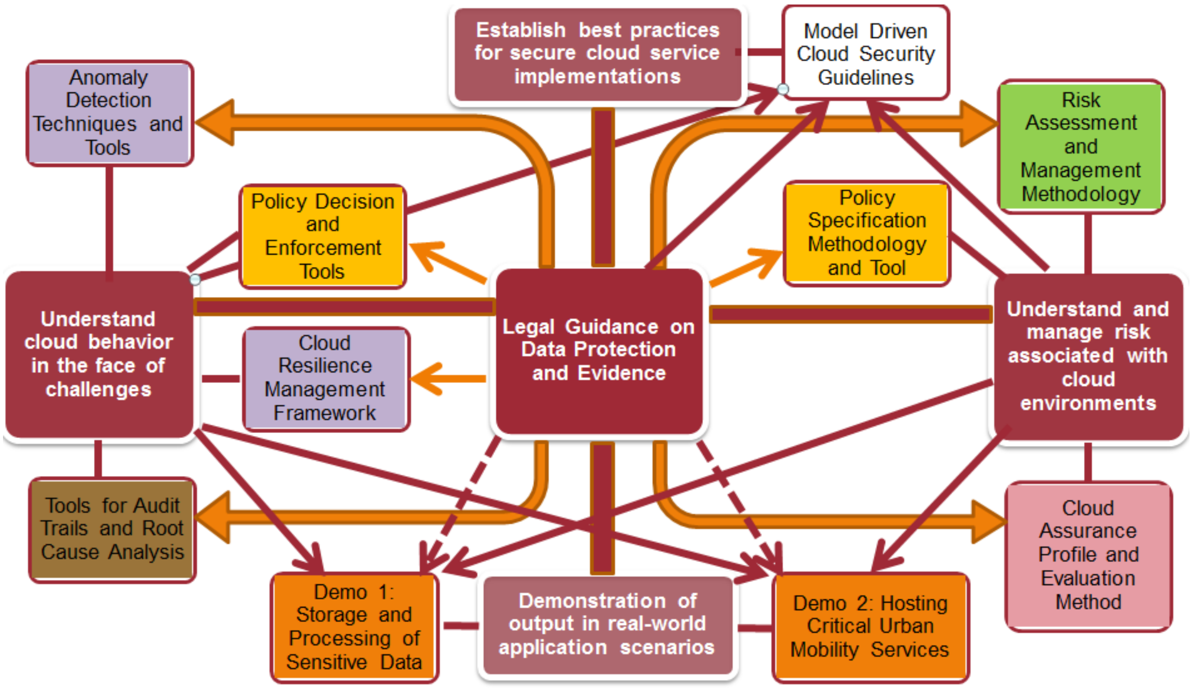
Establish best practices for secure cloud service implementations
Model Driven Cloud Security Guidelines
Anomaly Detection Techniques and Tools
Risk Assessment and Management Methodology
Policy Decision and Enforcement Tools
Policy Specification Methodology and Tool
Understand cloud behavior in the face of challenges
Legal Guidance on Data Protection and Evidence
Understand and manage risk associated with cloud environments
Cloud Resilience Management Framework
Tools for Audit Trails and Root Cause Analysis
Cloud Assurance Profile and Evaluation Method
Demo 1: Storage and Processing of Sensitive Data
Demonstration of output in real-world application scenarios
Demo 2: Hosting Critical Urban Mobility Services

FIGURE 3: LEGAL INFLUENCE OF TECHNICAL WORK

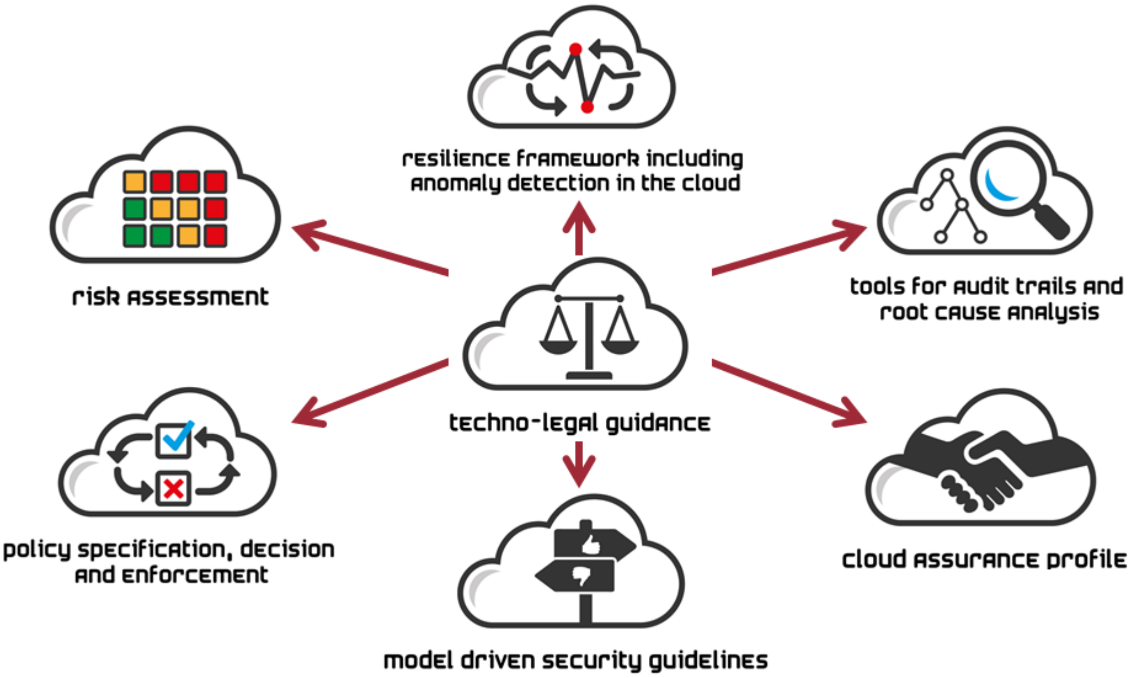
resilience framework including anomaly detection in the cloud
risk assessment
tools for audit trails and root cause analysis
techno-legal guidance
policy specification, decision and enforcement
cloud assurance profile
model driven security guidelines

FIGURE 4: RTD OUTPUTS

5.2 Risk Assessment

5.2.1 Scope and function

Deliverable D3.1 of the SECCRIT project describes different aspects and methodologies for risk assessment. A risk assessment approach that takes cloud related risks into account and enables a comparison between a cloud-based and a non-cloud-based solution is proposed in D3.1.

The first stage of this approach makes use of the Verinice Information Security Management System (ISMS) tool, which is a software that allows the user to define risk acceptance levels appropriate for their organization with regard to the risk categories confidentiality, integrity and availability.[134] Business processes to be scrutinized can then be modelled with the tool and ICT assets can be modelled and mapped to the defined processes. In a next step, risk scenarios must be modelled and associated with ICT assets in order to be then able to identify possible protection measures against any identified risks.

In order to include cloud specific threats into the risk assessment, a “Cloud adoption risk assessment extension” was developed[135] which allows to model cloud specific scenarios and related risks. This “SECCRIT vulnerability and threat catalogue” can be imported into the Verinice tool[136]. The steps necessary for a risk assessment are then repeated for the considered cloud integration scenario. First, the cloud deployment scenario has to be modelled. In a next step, existing risk scenarios must be re-evaluated with regard to the new potential system environment including cloud components. The fact that integration of cloud components may cause whole new cloud-specific vulnerabilities and threats makes it necessary to reconsider potential risks and add risk scenarios arising specifically from the use of cloud-based technologies, e.g. risks related to transmission of data over (public) networks to external data centres and processing of data in the realm of other providers. These additional risk scenarios could then be mapped again to ICT assets and risks and possible countermeasures can be analysed.

If both the risks of a traditional non-cloud environment and the risks after potential inclusion of cloud components have been analysed a comparison of risks can be conducted and advantages and disadvantages of cloud enhanced data processing can be weighed up against each other. The outcomes of risk assessment processes can then be used to support the decision whether or not to use cloud computing technologies, and how to protect data processing against both non-cloud-specific risks and additional potential cloud specific risks.

The results of the risk assessment are typically recorded in a document that can be automatically generated by the Verinice tool. This document can then be used internally within an organization to disseminate the results of the assessment, and to support strategic decision making about how to treat risks, and whether to migrate services to the Cloud. The document might be disseminated to those in a company that are dealing with operational aspects and higher-level management, e.g., a Chief Security Officer that makes strategic board-level decisions. In some cases, the information generated by the risk assessment process will be shared with external third-parties, e.g., to auditors as part of an ISO 27K certification process.

[134] SECCRIT Deliverable 3.1, section 7.2.1.
[135] SECCRIT Deliverable 3.1, page 49, section 7.2.2.
[136] SECCRIT Deliverable 3.1.

5.2.2 Legal aspects of risk assessment concerning liability / evidence law

Carrying out risk assessments can support the involved parties when it comes to identifying risks that are inherent to data processing and possible protection measures to mitigate or avoid any identified risks. The cloud adapted risk assessment method presented in D3.1 of the SECCRIT project can help to decide whether it is acceptable from a data security and data protection point of view to outsource certain data processing steps into a cloud environment. Furthermore, a careful risk assessment can help to determine the necessary security levels and measures to ensure them.

With regard to liability and evidence, a properly documented risk assessment may help the parties to document why certain security risks were seen as probable and which possible countermeasures have been deemed necessary to prevent these risks. When it comes to questions of liability, a party that has carried out a risk assessment may use the outcomes to show that probable risks along the data processing chain were correctly identified and addressed by implementation of appropriate and state-of-the-art countermeasures. This may help the respective party, at least in part, to prove that no negligence occurring in their sphere of responsibility has caused failure or damage.

Since risk assessment is, however, not suitable to conduct live monitoring of system configurations and activities, it cannot serve as a proof that certain security mechanisms were actually properly implemented and active at a certain point in time, e.g. while an attack or a system failure occurred. A risk assessment can therefore only serve as an indicator that certain security aspects have been identified and considered beforehand.

If a company has decided to outsource parts of its data processing to a cloud provider, the company may carry out a risk assessment with special regard to cloud specific risks and choose a provider who can provide systems fulfilling the security requirements deemed necessary according to the risk assessment. The outcomes of the risk assessment may then serve as a basis for choosing appropriate security levels and designing appropriate security policies to be used in order to ensure actual fulfilment of security requirements.

5.2.2.1 *Use for Mirasys Use Case Nr. 1*

Concerning the Mirasys use case Nr. 1 - the act of vandalism in the night - where the station was vandalized as no video images have been recorded the outcomes of the risk assessment could permit both the cloud user and the provider[137] to substantiate their case. As the provider could use the result to show that the system was not vulnerable at the time of the risk assessment, it could prove for that specific moment, that no fault and thus no negligent behaviour has been given. A negative outcome could in return indicate that no reasonable care has been exercised. For the user respectively, if he has knowledge about the vulnerability of the system and does not inform the provider or get in touch with him, this could also make the user himself as well acting negligent, especially if the documents concerning the risk assessment have been disclosed to him. It therefore highly depends on who has knowledge about the outcome of the risk assessment and in particular what was contractually owed. The provider might in return also act negligent if he does not react even though the risk assessment indicates a vulnerable system. This implies for the Mirasys use case, that the outcomes of the risk assessment could be highly valuable as they can permit an indication about the vulnerability of the system. If the system was therefore vulnerable, it seems probable that the provider acted negligent. The user would lose the

[137] He is thus not a respective party, but the user also needs to disprove the behaviour of the provider, therefore proofs concerning his behaviour are necessary.

lawsuit against MetroSub but win the subsequent lawsuit, if a third party notice was given against the provider.

5.2.3 Legal aspects of risk assessment concerning data protection law

Since the risk assessment described in D 3.1 is normally carried out in an abstract way without interfering with actual data processing systems and without use of actual data[138], there is little to no risk of data protection infringements in the course of the risk assessment procedure itself. Nonetheless, risk assessments are very important from a data protection point of view since they are crucial to ensure compliance with data protection law.

Data protection law obliges the controller to implement appropriate technical and organizational measures regarding security of processing, as stated in Art. 17 95/46/EC and the respective national implementations of the European data protection directive. This provision states, that personal data must be protected against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access and against any other unlawful form of processing. The level of security must be appropriate to the risks represented by the processing and the nature of the data to be protected with regard to state of the art and cost of implementation (Art. 17 of directive 95/46/EC). In case the controller involves other parties processing data on his behalf, the controller still remains responsible for choosing a processor providing sufficient guarantees with respect to technical and organizational measures and furthermore he is obliged to ensure compliance with these measures.

Similar obligations for both the controller and the processor can be found in Art. 30 (titled “Security of processing”) of the upcoming General Data Protection Regulation. This regulation assigns even greater significance to risk evaluation prior to processing of personal data by introducing in its Art. 33 a so-called “data protection impact assessment”, requiring the controller in certain cases to evaluate risks for the data subjects concerned and to name safeguards and security measures envisaged to ensure protection of personal data. Under the upcoming data protection regulation detailed data protection impact assessments may therefore become mandatory.

With regard to these obligations of the controller arising from current and upcoming data protection law, a (cloud specific) risk assessment procedure is a suitable means to identify the various risks that are represented by the processing of personal data and to decide what level of security is appropriate for the respective kind of processing. Since cloud computing may lead to additional risks inherent to cloud technologies, a risk assessment methodology must take these specific risks into account.

5.2.3.1 *Use for Mirasys Use Case Nr. 2*

The Mirasys use case Nr. 2 - the misbehaving politician - deals with data leakage questions. If a risk assessment would have been carried out, possibly it should have identified a vulnerable system which could be susceptible for data leakage. Therefore with this tool such data protection infringements could have been obviated. Thus this tool permits to enforce data protection requirements, like access control and helps to prevent risks.

5.2.4 Summary and legal recommendations

As the risk assessment tool permits to identify and prevent security risks, this is very helpful for identifying countermeasures. The risk assessment may thus help to fulfil and enforce the

[138] See Deliverable 3.1, p. 67.

requirements and obligations set by data protection legislation. Concerning Liability and Evidence Law the cloud user could indeed use the outcome of the risk assessment to indicate if a system was vulnerable or not. The existence of a vulnerability could then speak in favour of a negligent behaviour.

However, a continuous monitoring and risk assessment would be highly valuable, as the risk assessment by now is only permitting an on demand check, which is not foreseen constantly. Therefore it can only indicate the status of the system for a certain moment. It can, however, not indicate if countermeasures have taken place afterwards, which might then make the system secure again. It therefore only permits a specific check, which does only count for the moment it takes place and therefore only indicates the vulnerability in the time of the request.

5.3 Policy specification, decision and enforcement

5.3.1 Scope and Function

The Policy Specification, Decision and Enforcement output cluster is divided into Policy Specification Methodology and Tool and Policy Decision and Enforcement Tools.

In the Policy Specification Methodology and Tool activities, a methodology and tool framework were developed that improve the specification of security policies in terms of user experience. The two following research results were produced:

1. A general methodology for the systematic elicitation of security policies including their transformation into security policy templates that can be reused for a specific application domain and user group.
2. The PAP framework provides policy editors targeting at different user groups and application domains. It comprises different usability approaches and security policy specification paradigms for providing tailored guidance to the respective user group.

Both contributions aim to support the stakeholders (e.g., CI Service User, Cloud Infrastructure Operator) in the SECCRIT architectural framework to empower them to specify their security demands.

Policy Decision and Enforcement Tools activities focused on the development of concepts and technical solutions for policy enforcement in virtualization environments. The generic policy enforcement framework IND²UCE has been used and extended by appropriate enforcement components for cloud environments. The two extensions are:

1. Enforcement components for the Critical Infrastructure Service Level. We extended our policy enforcement framework to interact with a cloud storage service based on HBase and Hadoop.
2. Enforcement components for the Tenant Infrastructure Level and the Physical Cloud Infrastructure Level. We developed components to interact with the Cloud Infrastructure Management. It includes also a component to retrieve contextual information from the Cloud environment.

The enforcement components developed within the Policy Decision and Enforcement Tools activities can be used to enforce stakeholders' security demands that have been elicited and specified by using the methodology and tools developed in the Policy Specification Methodology and Tool activities. The extension of having a contextual information point allows the determination of location-related information during the decision making (e.g., the location of the physical hosts of a datacentre). However, the enforcement framework relies on the information provided by external components and cannot guarantee the exact location.

Security policies are an established instrument for specifying security demands. A security policy aims at protecting an asset. Security policy templates are a generic representation of a security demand in natural language that can be instantiated to formulate a concrete security demand as a security policy. Those security policies can be transformed into machine-readable security policies and then enforced by an appropriate security policy enforcement framework, such as the IND²UCE framework. Thus, the behaviour of the enforcement tools depends on the specified and deployed security policies.

Security policies can be specified by various stakeholders within the application domain. In case of cloud environments hosting critical IT services, that can be in theory all participants:

- **Cloud infrastructure operators** want to provide a basic set of security for their customers. Those policies mainly protect the integrity and availability of the whole cloud infrastructure.
- **Tenant operators** may want to even restrict the general security specifications of the cloud infrastructure providers to better fit the security expectations of their customers.
- **CI Service Providers** may want to customize security settings for their specific services. Security policies can be more fine-grained to adapt better to the security demands of the concrete service and its data. Especially usage control policies may only be specified starting at the level of services, as intended data usage depends on service, its owner and its users.
- **CI Service Users** may want to apply their own security demand on their data, before they release it into a cloud service. This especially applies to data related to critical infrastructures.

In general, the security policies that an individual stakeholder may want and is allowed to specify depend on the security demands of this stakeholder and the security policies that are already in place, created by stakeholders from higher architectural levels. The security policy specification possibilities are restricted by security policy templates. Those templates can be instantiated by all stakeholders or only specific ones (e.g. for stakeholders from one architectural level).

The stakeholder may be forced to specify security policies by the target system. This depends on the concrete implementation of the policy enforcement framework in the target system.

Each stakeholder is responsible for the content of his own specified security policies. But, the technical enforcement of those must be guaranteed by the operator or developer of the policy enforcement framework, which must correctly achieve the demanded security behaviour in the target system. If the correct enforcement of security policies in a target system is proven, the responsibility fully lies with the policy creator.

Service level agreements (SLA) cover security aspects in an organizational way. Some of those can be technically enforced by security policies.

The result of a policy enforcement can be seen as:

- the system and/or data state after the enforcement

- the system and/or data modification after the enforcement

Thus, policy enforcement results can be:

- the sum log entries that the IND²UCE framework is producing
- the data items that are controlled by the IND²UCE framework

The log entries of the IND²UCE components can be made available on request. There is no automatic notification. However, the policy creator is free to add notifications as part of the policy behaviour. Hence, the ability to send notifications after policy enforcements can freely be specified in the security policies and is supported by the IND²UE framework. . Notifications may include showing a message on the administrative interface or sending an email to responsible persons. In the context of SECCRIT, notification can be send via email, logged into a file or pushed to a demonstrator user interface.

5.3.2 Legal aspects of policy specification, decision and enforcement concerning liability / evidence law

Security policies as described in deliverable D3.2 of the SECCRIT project are an instrument to formulate security demands of end users regarding assets, where assets in the given context can either be sensitive data, critical infrastructure services or different parts of the virtual or physical cloud resources.[139] Each policy contains a threat description and a countermeasure to be applied in case the respective threat materializes.

Security policies can be laid down as binding agreements in Service Level Agreements. In order to ensure compliance with legal requirements of a technical system such as a cloud infrastructure with the respective security policies, a policy enforcement framework capable of interpreting and enforcing machine-readable versions of these policies can be implemented into the system. This tool can therefore be used to enforce legal requirements, like contractually given or prescribed by law.

As security policies can cover and address a wide range of requirements and issues in the sphere of different stakeholders and at different levels of the cloud architecture, it is difficult to generically analyse legal aspects concerning the use of policies and the policy enforcement framework. It therefore always depends on the specific case and on the particular needs of the respective parties. For that reason we will only concentrate on the function and the use of this tool in general without concretizing demands in detail.

In which ways policies influence data processing and related legal aspects depends on where policies are being used, which kinds of policies are specified, if policies are being technically enforced and how policy related events are being documented. In addition, the enforcement of policies may prevent violations or just detect them. Policies and measures induced by policies can be relevant for questions of liability as well as for evidence purposes.

The exemplary policy templates listed in D3.2 contains several examples of policies with possible relevance for liability and for providing evidence thereof.

Concerning liability different constellations can be identified which could play a role for attributing responsibility.

[139] See SECCRIT D3.1, Section 3.1.

These examples[140] are:

- The policy had to prevent a fault, however such a fault occurred and it caused damage. It is now questionable who had the responsibility to specify such a policy and whose fault it is that even though it was set up, a fault occurred. Within this constellation, the probability that a breach of duty was given is indeed very high. Generally it lies in the responsibility of the provider to ensure that the system fulfils the policy demands. It is therefore very likely that somehow some ongoing procedures managed to avoid this policy. This fact could speak in favour that the one who was responsible to ensure the correct execution of the respective policy did not exercise reasonable care. Therefore, the responsibility in this case lies very likely in the sphere of the operator, as he is the one who has to ensure that specified policies are enforced properly. Concerning the developer of the policy enforcement framework, he is the one on which the provider relies in order to fulfil his duty of enforcing set policies. Within this constellation he has to be considered as a person who is used to fulfil the duties of the obligor, thus the provider. The provider would hence be responsible for his behaviour. If he therefore sets up a non-well-functioning policy enforcement framework, the provider will be the one who will have to take responsibility for this, as he is relying on him (external relationship). In turn he can take recourse on the framework developer (internal relationship).

- The policy specification was wrongfully created and due to this a fault occurred. The responsibility would in this case lie with the policy creator.

- A fault occurred, there was no policy set up, however if this would have been the case, the fault could have been prevented. The responsibility in this case would lie in the sphere of the one who had the duty to create the policies. This fact can very easily be used for providers for example to shift their responsibility in contractually specifying that the cloud user can use this tool to concretize his security demands. In so doing, it will be the own fault of the cloud user, if he misses to set up such policies. Policies may, to some part, therefore shift responsibilities between the stakeholders involved in a multi-layered cloud architecture. An involved stakeholder (e.g. the critical infrastructure service provider) may implement a policy enforcement framework within his systems and then provide his users with the possibility to define the security policies tailored to their specific needs themselves. In this case, responsibilities that would normally lie with the provider could be transferred to the user, who gains more control over details of security measures, but on the other hand bears accordingly greater responsibility. With regard to possible shifting of responsibilities and in order to avoid accidental security gaps or unintentionally low security settings, contractual agreements should very clearly address these aspects. It should be clear to all involved parties which security measures are already set as default at the architectural level in question or at higher levels. Especially critical infrastructure providers should very well know what kind of security measures are needed and either contractually impose the cloud provider to ensure these measures or make sure that they take responsibility on their own for this. Mostly it is recommended for the cloud users to specify their security demands and impose the duty of ensuring that the system fulfils them properly on the cloud provider. The cloud provider would in that case be the policy creator and in the same time the operator. Closely related to this, is therefore also that the provider clearly defines what the policy framework can do, what are the limits of it and what security demands therefore the user can specify. Besides, the contractual regulation should

[140] We are considering especially theoretical occurring faults – some of these faults might technically not really seem to be probable, but however in order to ensure completeness we want to show the different responsibility possibilities.

also state how policies and policy enforcement can be supervised and documented in a running system, in particular if it is intended that the user can check if the policies he provided/demanded are actually working and how actions with regard to policies are recorded to log files or audit trails.

The responsibility lies therefore either in the sphere of the policy creator, which can depending on the contractual obligation be the cloud user or the cloud provider and concerning the enforcement responsibility will be imposed on the provider.

The tool is also valuable for strengthening the legal position of both parties in lawsuit constellations. Especially the fact that the log entries of the IND²UCE components can be made available, presents an interesting opportunity to provide both parties with equal starting positions in court. The contractual obligation should therefore define that the cloud user has to receive continuous notifications, especially in the cases when the policy enforcement has been realized. The way of notification as email, logged into a file or pushed to a demonstrator user interface is for instance not significant as long as it is ensured that it comes from the "creator" and has not been modified until it reached the addressee. As the court is free to assess and judge the evidence the court therefore needs to be convinced that the content corresponds to the truth. This data should therefore be collected and stored in a tamper proof way and it should be accessible for the stakeholders who may need it as evidence.

As generally automatically enforced policies can help to ensure the fulfilment of contractual and legal obligations and to avoid damages, the fact that no fault occurred speaks also in favour of a proper functioning of the system and thus a non-default of the provider. The provider could therefore show with respective log files that the system worked properly and that he thus exercised reasonable care as the policy enforcement framework shows that the system fulfilled the desired security demands. Several of the example policies foresee a notification feature or deal with provision and recording of log information to audit trails. Some of the policies laid out in D4.2 deal for example with shortfalls of resources (e.g. policies CI5, CI6, CI8), attack scenarios (e.g. CI4, CI11, TI2) or possible hardware failures (e.g. policies ….). Policies that are used to detect and resolve a shortfall in physical or virtual resources may for example be used by the providers of the physical infrastructure and the tenant infrastructure in order to ensure provision of sufficient resources according to their respective contractual obligations at all times. If these policies also provide logging information about the problem and the measures undertaken to resolve it, the respective party may use this information as evidence in order to proof that sufficient resources were provided and the contractual obligations have been met at the time a problem occurred. Policies that provide log entries of certain events may therefore help in various ways to clear up responsibilities in the aftermath of an event that has caused damages.

The contract should therefore ensure that the cloud user receives notifications.

5.3.2.1 *Use for Mirasys Use Case Nr.1*

This tool improves the proving situation of the cloud provider and the cloud user. Within the Mirasys Use Case Nr.1 – the act of vandalism in the night - we came to the result that the user needs to prove the provider's fault in order to lose the first case and win the subsequent one.

The policy specification, decision and enforcement tool could be valuable for the cloud user, as he could use the notification as a proof in court for substantiating his case, independent if it is an email, logged into a file or pushed to a demonstrator user interface. With these notifications he could probably show that a fault occurred. This indirectly also influences the default as the fact that a fault occurred makes it very probable that a negligent behaviour has been exercised. In particular if the SLA's state that such a behaviour had to be obviated and the responsibility for this lies in the sphere of the provider, the cloud user could with these notifications prove the fault. Still the court will need to freely assess if negligence was given, but with the additional expert evidence the cloud user could provide the most probable reason and thus sufficient proofs for the default of the provider. Consequently the cloud user could prove the provider's fault, lose the first lawsuit and win the second one. However only with this tool, other probable reasons for the non-functioning of the system could possibly also be given. Therefore the provider could indeed prove easily with other internal management data a proper behaviour. The cloud user might possibly need other tools (which are developed within SECCRIT) to substantiate his case even more strongly.

The provider on his turn can also show a proper behaviour, if the policy framework worked properly and no threat has been reported. He can further on use the contract to show that he has not been the one who had to create the policies. Moreover he can use the tool for proving compliance with the SLA's and thus the contractual obligation he has been subject to. Besides he will also have to prove with other proofs, like witnesses, that he adequately enlightened the cloud user about the limits of the tool.

This tool is therefore useful for proving the fault and SLA compliance.

5.3.3 Legal aspects of policy specification, decision and enforcement concerning data protection law

Depending on the specific policies in use in a cloud environment, policies may also have an impact on data protection related issues. Even if policies themselves do not use personal data, they may influence the way personal data is handled[141] and therefore aspects of data protection must also be taken into account. The impact of policies and policy enforcement technologies on data protection issues is difficult to analyse generically from a legal point of view since policies can be used to address a wide range of different trigger events and possible measures.

As stated in Art. 17 95/46/EC, controllers and processors handling personal data are obliged to ensure security of processing: "*Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.*" The upcoming data protection directive will most probably set comparable requirements in its Art. 30.

Policies can, amongst other purposes, be used to detect, report and avert impending or already materialised risks concerning the security of processing either in general or even with specific regard to requirements originating from data protection law. Some of the exemplary security policy templates listed in deliverable D3.2 of the SECCRIT project are suitable to give an insight on how policies may have an impact on data protection critical issues. Policy TI13, for example, can be used to ensure that sensitive data is securely erased, policy SP1 can prevent leakage of classified data and policy SU1 can inhibit the transmission of sensitive data outside defined jurisdiction areas. The influence of policies on data protection is, however, not limited to the policies specifically intended to ensure data protection. Nearly every policy that influences

[141] See D3.2.

processing of (personal) data may potentially also have an impact on data protection requirements.
The tool is therefore useful either for enforcing data protection regulations but also for ensuring the requirements prescribed by law.

5.3.3.1.1 Use for Mirasys Use Case Nr. 2

Within the data protection section we came up to the result that especially the transparency principle is often infringed in cloud scenarios and that the cloud user can neither fulfil the data subject's rights properly nor can he control the cloud provider. With the Mirasys Use Case Nr. 2 – the misbehaving politician, the data of the data subject (stored in a cloud system) were leaked and somehow appeared in the newspaper. This case is an example that the cloud user does not know what actually happens with the outsourced data and that the provider could use the data for example for own purposes which the cloud user (generally) will not have knowledge about. The lack of control and transparency is especially for the data subject very inconvenient. With the policy specification, decision and enforcement tool control and transparency are in a way also addressed.

Especially the fact that the cloud user can get notifications about the proper execution of security demands, permits him a "real" control option. He can check if the cloud provider fulfils set up requirements which should also reflect the data protection regulations, especially concerning the appropriate technical and organizational measures. Policies should also be used for ensuring that only authorized parties can access the hosted data.

Fulfilling the access rights of the data subject will thus not guarantee that the actual "answer" of the tool matches the real givens. The contextual information point allows indeed the determination of location-related information during the decision making, like for example the location of the physical hosts of a datacentre, but this information relies on external components which cannot guarantee the exact location.

The opportunities of this tool permit the cloud user to set up security demands and to check their correct fulfilment. It can to a certain degree, also permit to fulfil data subject's rights by showing them the notification about where the location of data is, if data have been erased etc.
The cloud user needs to ensure contractually that he gets respective notifications about the result of the policy enforcement, like for example ensuring that data are located in desired locations.

Therefore, if within this tool a policy would have been established, which ensures that the employees of the provider or other non-authorized persons cannot access the outsourced data, publishing of the image of the vomiting politician in the newspaper could have been prevented.

5.3.4 Summary and legal recommendations

To sum up, policies and policy enforcement mechanisms offer a wide range possibilities to control and document system behaviour.
Seen from the perspective of liability and evidence law, enforced policies can help to avoid cases of damages and liability as well as they can help to gather evidence in case an incident occurs.
Policies can be used in a targeted way to help ensure and improve compliance with data protection requirements through direct actions as well as through information and documentation

of data processing. Any policies aiming mainly at purposes other than data protection should still be thoroughly checked for possible side effects concerning data protection issues. In many cases, the main responsibility for compliance with data protection requirements lies with the cloud user. He should therefore ensure that such policies reflect the data protection regulations.

Since policies can be used at various architectural levels and by various stakeholders, responsibilities should be clearly defined contractually according to the needs of the involved parties. It is recommended for the cloud users to specify their security demands and impose the duty of ensuring that the system fulfils them properly on the cloud provider.

5.4 Resilience Framework including anomaly detection in the cloud

5.4.1 Scope and function

The term resilience describes the ability of a system to provide and maintain an acceptable level of service even when facing challenges[142] such as technical failures or attacks.

Deliverable 4.2 of the SECCRIT project describes a cloud resilience management framework (CRMF) which implements various mechanisms to improve resilience within cloud environments. In the following some legal aspects originating from the fields of evidence law and data protection law will be considered with regard to the CRMF.

The CRMF consists of two main functions interacting with each other, the *Deployment Function* and the *Resilience Manager*, each of which consist of several sub-components.[143]

The deployment function is part of the Tenant Infrastructure Management System (TIMS) and is responsible for providing the Cloud Infrastructure Manager with configurations for creation and deployment of virtual machines that are to be used for the critical infrastructure[144].

The sub-components forming the deployment function are the SLA parser (responsible for extracting the respective requirements from SLAs or service descriptions), the placement function (responsible for mapping the requirements to the physical cloud infrastructure) and the deployment template generator (responsible for generating templates that are processable by the respective cloud management system)[145].

The other main function of the CRMF is the Resilience Manager consisting of several instances running at different cloud infrastructure nodes, each of these RM-instances being composed of the following three sub-components: *Anomaly Detection Engine* (ADE), *Policy Engine* (PE) *Coordination and Organization Engine* (Coe)[146]. The instances of the Resilience Manager can gather and analyse data from their local cloud infrastructure node and their network view and they are also able to communicate with other RMs through the Coordination and Organization engines of the different RMs, thus forming a distributed resilience management system.

The anomaly detection engine is comprised of three sub-components: The Data Collection Engine (DCE), the System Analysis Engine (SAE) and the Network Analysis Engine (NAE), which collect and analyse data in order to detect anomalous behaviour or events which can subsequently be analysed by the Fine Grain Analysis (FGA) in order to identify causes for anomalies and locate them.

Reactions to challenges that are detected by the monitoring mechanisms are then selected and executed by the Policy Engine, which uses predefined policies in order to take appropriate action

[142] See D4.2, Section 2.3
[143] See D4.2, Section 3.1, p.19.
[144] D4.2, Section 3.2, p.22.
[145] D4.2, p.23ff.
[146] See D4.2, Section 3.1, p.20.

to solve or remediate the detected problems. The IND^{2}UCE policy engine used in SECCRIT is based on an Event-Condition-Action (ECA) approach, meaning a certain event (*trigger*) leads to the verification of a certain condition and depending on the outcome the desired action is performed[147]. The policies specifying these rules can either be preventive or of a mere detective nature. Preventive policies can perform direct actions in order to prevent certain processes already in the first place, whereas detective policies only report policy violations and may enable or induce measures in the aftermath of a policy violation which already occurred[148].

5.4.2 Legal aspects of resilience management and anomaly detection concerning liability / evidence law

The contract between cloud user and cloud provider may stipulate certain requirements for the cloud resources to be provided for the fulfilment of the contract. The cloud user may for example demand placement of virtual resources within certain jurisdictions in order to comply with data protection legislation, he may require certain redundancy levels or (anti-)affinity of certain virtual resources or placement only on hosts which fulfil specified security requirements. Deployment function and resilience management have a direct impact on placement, availability and security of virtual resources. Virtual resources must be allocated in accordance with contractual and legal obligations in the first place and any changes (e.g. deployment of new VMs or migration of existing VMs) must also be carried out in accordance with these obligations. Deployment templates and resilience policies must therefore be designed and chosen carefully and with due respect to the respective contractual and legal requirements the owed cloud environment is subject to.

Hence in case of a dispute, the question whether contractually set conditions and legal obligations have been met at all times may depend on actions performed by components of the resilience management framework. Misconfiguration of virtual resources may lead for example to failure or malfunctioning of the services they are provided for or to data protection violations due to misplacement of virtual resources. Especially a non-resilient system could possibly be an indication of a negligent behaviour, as the provider’s duty consists in providing a functioning system.

In case of a legal dispute both parties may be in need of proof to clarify who was responsible for failure or malfunctioning. The cloud user may, for example, want to prove that the cloud provider did commit a breach of duty, whereas the cloud provider may want to prove that he did fulfil all contractual obligations and that neither he nor anyone acting on his behalf did act deliberately or negligently regarding the failure. Activities of the resilience management framework which may be relevant for questions of liability should therefore be documented in a way sufficing for the respective party to serve as proof in court[149]. Since the tools for audit trails and root cause analysis[150] are already intended to gather various information it might be reasonable to transmit information from the resilience management framework to the transparency enhancement framework in order to provide a holistic view of system activities.

Anomaly detection may also play an important role in terms of liability and aspects of evidence law. The anomaly detection engine and its subcomponents are intended to detect anomalous system behaviour resulting from challenges the system is facing.

[147] See D4.2, p.24, p.27.
[148] See Seccrit Deliverable D4.2, Section 3.4.2, p.26.
[149] For details see section 3.
[150] See 5.5.

Anomaly detection and the possibility to induce countermeasures may be part of the contractual obligations a stakeholder is supposed to fulfil. A minimum level of security and resilience may be owed even without an explicit agreement[151], but especially when the security of a critical infrastructure is at stake, the parties will probably in most cases have contractually agreed upon certain security levels to be fulfilled. Providing anomaly detection mechanism may therefore, depending on the specific case, be part of the obligations a stakeholder has to fulfil and failing to provide it may in these cases be an indication of fault on the side of this stakeholder.

Furthermore, output from anomaly detection may serve as evidence in different ways. First and most obvious, recorded output may serve as proof that anomaly detection was available and functioning correctly at the time a challenge occurred. Depending on the specific case, recorded output from anomaly detection may also be used as proof that a challenge occurred and in some cases the logged data may even help to elucidate the nature or causes of an incident. In so doing it could probably be determined if the respective party exercised reasonable care and thus did not act negligent even though a challenge occurred. Additionally the reaction of the cloud user after an event is also of strong importance, as the cloud provider can then act negligent (and thus not be responsible for the event itself, but for the implications afterwards due to a non-acting) if he does not take appropriate actions for removing bugs, deploying counter-measures etc. Such records might therefore also be valuable in matters of evidence. Recorded output from anomaly detection could for example be used in a court debate as evidence in the form of legal inspection or as part of assessments in the course of expert evidence.

5.4.2.1 *Use for Mirasys Use Case Nr. 1*

Within the Mirasys Use Case the outcomes of the anomaly detection could be highly valuable as they could help the cloud user to determine the cause of the fault (no record of video images). The expert could then analyse the records and conclude in his report, who is responsible for the occurred fault. As the court can assess this report freely, it will however in most cases follow the conclusions of the expert and recognize a default of the provider, if records show the fault and thus the negligent behaviour which caused it. Possible breach of duty in those cases could either be an acting which caused the fault directly or a non-acting especially in the aftermath of an event, if the provider failed to take appropriate measures to remove the bug. Therefore the Resilience framework and especially the anomaly detection can help to prove a respective fault and default and help the cloud user in this particular case to disprove the non-default of the provider. The cloud user therefore will lose the first case and could with such outcomes win the second one against the provider.

5.4.3 Legal aspects of resilience management and anomaly detection concerning data protection law

Since both the deployment function and the resilience manager have an influence on deployment, placement and protection level of virtual machines, aspects of data protection might become relevant, depending on the specific actions carried out by these components. Data protection issues may for example arise if virtual machines are placed on hosts outside specified areas (e.g. outside the European Union) or on hosts that do not fulfil specific security requirements. Deployment function and resilience manager depend on and act according to

[151] For details see section 3.5.1.2.

information previously fed to the systems in the form of service descriptions (deployment function)[152] and resilience policies (resilience manager)[153] which makes it important to ensure sufficient consideration of possible data protection impacts already in the course of designing service descriptions and resilience policies. Data protection impacts of deployment function and resilience manager depend on the specific case and are therefore difficult to analyse generically from a legal point of view. Both functions can be useful to help ensure proper fulfilment of data protection requirements by assuring that resource management is carried out in compliance with data protection requirements but they can also pose a danger to data protection if configuration data or policies supplied to these systems do not take due account of possible data protection infringements.

The Anomaly Detection Engine and its related subcomponents survey various system components and parameters as well as network traffic in order to detect anomalous behaviour that might indicate i.e. system failures or attacks. Network traffic being monitored in the course of anomaly detection may contain personal data regardless of whether personal data is required to perform anomaly detection.[154] Even if personal data that is analysed in the course of anomaly detection is discarded, deleted or reduced to inferred data that does not contain personal data anymore, personal data may be gathered and processed at least in the first place[155]. Special regard to data protection requirements is necessary were data collected by the anomaly detection engine is kept for later analysis, as far as this data may contain personal data which is subject to data protection laws.

Any processing of personal data must be justified under one of the justifications laid out in data protection law (Art. 7 95/46/EC). One possible justification for data processing is the necessity of processing in order to comply with legal obligations the controller is subject to (Art. 7(c) EDPD). Art. 17 95/46/EC binds the member states to oblige the 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, in particular where the processing involves the transmission of data over a network* […]". Anomaly detection and resilience management serve the purpose to survey and maintain correct functioning of the cloud environment by detecting anomalous system behaviour resulting from failures or attacks and their implementation may hence be seen as part of the technical measures intended to guarantee security of processing.

5.4.3.1 *Use for Mirasys Use Case Nr. 2*

The Mirasys Use Case shows in particular the problem, that it is not clear what the provider is doing with the outsourced data. In particular if the provider starts to use the data for own purposes he is required to have an own legitimation, either the consent from the data subject or a legal basis. With regard to data protection the resilience framework may at least be useful if the data leak was caused by a hacker as this RTD output has the scope to maintain correct functioning of the cloud environment by detecting anomalous system behaviour resulting from failures or attacks. Therefore it might be useful for preventing such a data leak if appropriate measures are taken in the course of an event, obviating that data are leaked by non-authorized (or even authorized) persons.

[152] See D4.2, Section 3.2.
[153] See D4.2, Section 3.2.
[154] See D4.2, Section 1.4.
[155] See D4.2, Section 1.3, page 9.

5.4.4 Summary and legal recommendations

The resilience framework and in particular the anomaly detection are very valuable especially for determining the cause of an event and attributing a possible negligent behaviour. Such activities of the resilience management framework should therefore be documented in order to be analysable by an expert in court. With regard to data protection measures carried out by the resilience framework in order to maintain a functioning system must ensure compliance with data protection requirements.

5.5 Tools for audit trails and root cause analysis

5.5.1 Scope and Function

The Tools for Audit Trails and Root Cause Analysis (TAT) activity achieved two main outputs: an independent transparency as a service framework called *CloudInspector* and a reliable audit trail storage called *Hybris,* which tolerates arbitrary server failures. The main objective was to enable tenants to get a view on processes inside the otherwise opaque cloud as well as to provide the opportunity to securely and reliable gather and store evidences of cloud operations and processes inside the cloud, in case of infrastructure as a service.

Thus the tenant can get information he cannot already gather by himself, i.e., TAT do not gather information from within the tenant's VMs, because this information is already available to the tenant and thus transparent anyway. Instead, TAT is focused to uncover cloud management system failures and thus to increase the transparency of the cloud. A major feature of the CloudInspector approach is that it works as independently from the cloud management system as possible, thus providing an independent view on the current state of the tenant's virtual resources within the cloud. Therefore, negligent behaviour of a cloud provider or cloud management software failures should be detectable. However, TAT is not able to unveil every case of wilful misbehaviour of the cloud provider. This output cluster provides tenants with auditable information in real-time about their deployment in the virtualized infrastructure of the cloud provider as well as the possibility to collect evidences for a later Root Cause Analysis in court, similar to black boxes used in airplanes to support investigations after a plane crash.

More specifically, the collected information is gathered independently from the cloud management system on the physical machines of the cloud provider and thus provides a view on the interactions between the tenant's virtual machines and these physical machines. Examples for such information are whether the tenant machines are co-located or on separate physical hosts, or whether VMs from other tenants are placed on the same physical host, posing a potential security risk, or in which country virtual machines are placed. Users of TAT (tenants of a cloud provider) are able to run on-demand checks of contractual agreements (civil law) or may exercise their right of access (data protection law). Moreover, audit trails are continuously collected and stored, e.g., by a trusted third party which uses Hybris to store data in a reliable and secure way. This storage solution allows for a configurable degree of protection against malicious storage nodes, i.e., nodes where false information can be inserted or correct logs may be deleted, and at the same time remains efficient in terms of overhead and latency. The implementation of Hybris even allows for the use of public clouds as individual storage locations, under the assumption that the entity responsible for storing the audit trails (here a TTP) has a private and trusted environment where to store for example encryption keys.

In case of a debate in court these stored audit trails could be used to determine if the cloud provider has fulfilled its due diligence (by legal inspection and legal expert). While users of TAT (tenants of a cloud provider) itself are able to run on-demand checks in real-time, continuous stored audit trails can be managed in a way so that they are only accessible by legal experts and persisted at a trusted third party (trusted by tenant and cloud provider).

Monitoring agents called Transparency Enhancement Modules (TEM) are placed in the physical cloud infrastructure. They gather information, either on-demand or continuously, that is provided to the tenant either directly via a Transparency Controller Module (TCM) or that is stored as audit trails for later analysis via a Logging Aggregation Module (LAM), handing it over to a TTP which uses a trusted and highly available storage such as Hybris (for more details see D5.3). Information gathering works using libraries and functions available on the physical hosts. An example list of these functions and a definition of the API can be found in the updated version of D5.1. They can be grouped into the categories Hardware, Software, Operating System and Hypervisor, where all of them refer to the physical host itself, not to internals of VMs instantiated on the physical host.

The result, i.e., the gathered audit information, is first of all stored on the individual TEMs. It can then be provided directly on-demand to the tenant via the TCM, or it can be handed over to a TTP and logged to create an audit trail by storing it reliably and with a manageable degree of trustworthiness. The first option would typically happen if the tenant has actively requested audit information, then the tenant would simply get an immediate response (if the requested property is currently fulfilled) to his request (a request possibly meaning using a specific web page). The second option would mean a continuous storage of logs by a TTP, where a notification for each stored item might not be useful, except for highly critical events. It could, however, be possible to report, e.g., the number or frequency of stored logs in daily, weekly or monthly reports (not part of the research output). Audit trails are stored at a TTP in a tamper-resistant way (with support of Hybris). In addition, the audit trails may be encrypted even before being handed over to the TTP, ensuring that this party cannot access the logs without the according keys, which should be held by the tenant and the cloud provider.

In the first case (on-demand checks), it would principally be the tenant getting this information, although a trusted auditor or the cloud provider might also be able to run checks. In the second case (evidence), audit trails will be maintained and protected by a TTP and may be handed over for legal inspection to an expert in court.

5.5.2 Legal aspects of tools for audit trails and root cause analysis concerning liability / evidence law

With regard to the chosen architectural framework (Fig. 1) the *CloudInspector* is placed on the physical cloud infrastructure level and thus provides a very promising way of strengthening the legal position of the other actors on the other levels in a respective lawsuit. As the CI Service user on the top level of the architectural framework is the controller, he has the responsibility to fulfil the data subject's rights. The CI Service Provider who manages the resources has to be considered as the processor, whereas the Tenant Infrastructure Provider and the Cloud Infrastructure Provider have to be considered as the subcontractors of the processor (CI Service Provider). The CI Service user therefore also needs to fulfil his control rights against the Tenant Infrastructure Provider and the Cloud Infrastructure Provider. As the *CloudInspector* permits an inside view of the physical infrastructure system a respective fault of the cloud infrastructure provider can be determined for which the CI Service User on the top level would be responsible as the responsibility is even given in chained relationships and also for subcontractors of the subcontractor[156]. The data which are therefore stored at a TTP could not only be used within the tenant and cloud infrastructure contractual relationship but can as well be disclosed within other (higher) contractual level relationships.

By breaking through the opacity, TATs are thus not only able to provide the tenant with the information he needs for substantiating his case but also the other occurring parties like the cloud user through the TTP. Not only the tools for audit trails can help to elucidate the fault and default of the cloud infrastructure provider, they can simultaneously also collect proofs (which are non-tampered stored at a TTP).

They therefore provide the tenant with a neutral way of getting an inside-view in internal processing mechanisms. The cloud provider does not have to fear that internal competitive fact and business secrets are disclosed, as the TTP stores audit trails only in an encrypted way. Additionally, a possible manipulation of data can be prohibited, as data are already transferred into the sphere of a TTP. By this it is already ensured that the cloud infrastructure provider cannot manipulate the files afterwards, as a system image of past activities is already given (ensured by a TTP). The audit trails will by this in most cases also record the possible negligent behaviour which enabled the fault, as the *CloudInspector* is gathering in a comprehensive manner and in real-time information of the interactions between the tenant's virtual machines and the physical machines of the provider. If a fault occurred which led to damage it still remains unclear if a negligent behaviour has caused it. The audit trails can therefore be useful to find out what the provider did in the past (root cause analysis). The link to the fault and the behaviour before therefore permits to identify a possible default. It can in turn also permit to show that the provider exercised reasonable care if the causality with the behaviour and the fault is not given. The TAT are therefore also valuable for the provider himself, as they permit as well to show a non-default and thus do gather also proofs helping the provider himself to substantiate his case.

In a respective lawsuit (tenant against cloud provider), the information gathered by the *CloudInspector* needs to be analysed by an expert. Within its report, the expert will either come to the conclusion that the fault was caused due to a negligent behaviour or respectively was not. Beside the analysis of the files and deducing from this the cause and negligent behaviour, the expert will also have to address the question if these data are non-tampered. As, however, the audit trails are time stamped they can at least not have been falsified when they have been created and transferred to a TTP.

The audit trails therefore need to be designed in a way that they permit a root cause analysis and thus can retrace the cause of a failure by simultaneously being non-tampered. This has already been intended in the development of the tool and is fulfilled by the *CloudInspector*. The judge will afterwards assess this proof freely and will in most cases follow the conclusions of the expert, as the judge does not have the particular expertise to assess the case on his own.

As audit trails are stored at a TTP they are not introduced by a process party which could have falsified the data in their favour afterwards. The TTP can be a witness and can report on how they stored the data (*Hybris* for example). The storage of those files in a tamper-resistant way by *Hybris* permits that data are not changed afterwards and therefore still ensures a system image at the time it has been produced. Encrypting the data before transferring them is helpful to ensure that the TTP only fulfils their duty of safekeeping the data without having access to the content and possibly manipulating it. Hybris therefore ensures that the transferred and received data are not falsified.

[156] See 3.5.1.3.

The combination of the *CloudInspector* and *Hybris* is therefore very valuable, as the *CloudInspector* gathers information which reflects the system status at the time it has been produced whereas *Hybris* (run by TTP) guarantees that these transferred data have not been falsified or deleted afterwards and still represents the already recorded system image. A continuous monitoring and information gathering of the current state of the tenant's virtual resources within the cloud can thus guarantee that it detects negligent behaviour of a cloud provider or cloud management software failure. On demand requests can additionally help the tenant to see what is going on and especially after a failure to get an inside view into internal operation mechanisms which might have caused the failure. This can help the tenant to gain a better understanding if he had damage, about asserting a claim and his chances of success. As for now the current legal situation would have led to the fact that the cloud user has practically no chance to prove the provider's fault with the consequence that a claim wouldn't be successful.[157] Consequently, these two tools enable real inside view and thus an improvement of the opportunities of the tenant and the cloud user, due to the gathering of information at the TTP.

The fact that the *CloudInspector* permits to fulfil both on demand requests and continuous monitoring ensures complete collection of data about relevant processes. These two monitoring possibilities include all necessary measures for permitting the cloud user or tenant to have an equal starting position with the cloud provider in a respective process.

Additionally, it might also be worth to think about gathering information about the behaviour of the tenant and the cloud user. This could permit the user in a respective process to show that he himself has not caused the failure and that he has not committed an own default. This is by now not foreseen by the *CloudInspector*. Protocoling the behaviour of the cloud user/tenant could show that they did not do anything related to the failure which finally caused the damage. However such a tracing should be very carefully effectuated in order to ensure that no rights respectively data protection rights of the cloud user/tenant are infringed.

5.5.2.1 *Use for Mirasys Use Case Nr. 1*

With the TAT the cloud user could provide independent proofs and thus disprove a non-default of the provider (if the provider committed the fault). By this he could lose the process against MetroSub and win the second one against the cloud provider who committed the breach of duty. Additionally the cloud provider could as well also use the gathered information to show that he exercised reasonable care. With the expert evidence, legal inspection and witness (Trusted Third Party) the audit trails can be analysed concerning their content and authenticity.

5.5.3 Legal aspects of audit trails and root cause analysis concerning data protection law

With regard to data protection law we need to distinguish between the outsourced data which could be personal data and the data gathered by the TEM, which in return should not contain any personal data[158]. Further on we have to distinguish between requirements which the *CloudInspector* needs to fulfil in order to be himself data protection friendly and data protection requirements which can be fulfilled due to the use of the *CloudInspector* (rights of the data

[157] For instance in Germany, the jurisprudence had since now no cloud specific case to decide. Most cases are extrajudicial arrangements.

[158] S. Section 3.11.1.2.

subjects). Additionally it can be used for enforcing data protection requirements (checking that technical and organizational measures are fulfilled).

The TEM is therefore very useful for breaking through the lack of transparency and control.

5.5.3.1 *Outsourced data*

As, however, the TEM is only focused on gathering information concerning the interactions between the tenant's virtual machines and the physical machines of the provider, direct actions concerning outsourced data are not gathered. As the *CloudInspector* is able to monitor what happens to virtual resources which may contain personal data and it is placed on the infrastructure level it is, however, not intended to have a direct look on outsourced data. It would thus be important to develop additional tools which also concentrate on the tenants and the CI Service Provider level. For example access rights of these data should also be gathered in order to provide the cloud user with a full inside view about activities which affect his outsourced data. The transparency principle especially addresses the lack of knowledge about the handling of personal data, which is particularly in cloud computing scenarios difficult to fulfil, as it is unclear for the cloud user if the provider possibly also accesses the data. Such accesses or modifications of data should therefore also be recorded (by additional tools) in order to permit the cloud user a transparent view on a possible handling of his data by any unauthorized person.

5.5.3.2 *Internal management data*

With regard to the data which the *CloudInspector tool itself* gathers it is mandatory that these data do not contain any personal data, especially of the employees of the provider or tenants. For evidence reasons it is sufficient to have audit trails which permit the attribution of the fault to the entity of the provider (no information about the concrete employee who might have committed a breach of duty is needed).[159] Furthermore, by using strong encryption before transferring audit trails to a TTP it is ensured that the data do not contain any personal data. Otherwise this would require a legitimation from the data subject, thus the employee of the cloud provider or tenant. Therefore transferring the data to the TTP does not represent a data protection case as the audit trails are not personal data. Encrypting the data before the transfer is therefore from a data protection view not necessary as no personal data are outsourced. The encryption is however necessary for ensuring that no modification thus a manipulation of the original data has been conducted.

5.5.3.3 *Fulfilling data protection requirements*

With regard to the requirements which the cloud user as a controller has to fulfil the *CloudInspector* is also useful. It enables the tenant to make on demand checks. He can by this assist the cloud user to fulfil the data subject's rights. However, as the TEM does not collect information about the outsourced data directly, the fulfilment can only be conducted indirectly. This means that the information the user gets on his request concerning the location of the data, is the information about the location of the virtual machine, respectively on which country the "physical" machine is located. The TEM cannot check whether a particular data set is actually stored in a particular virtual machine. This information would need to be extracted from information of the tenant about the internal processes of their virtualized system.

In contrast to the access rights, other rights of the data subject like correction, deletion or blocking do focus on the outsourced personal data directly. The record of modification of data, deletion

[159] See for more details section 3.11.1.2.

and blocking is however not foreseen by now by the TEM, as gathered information only relates to the status of the machines themselves. Other tools are therefore also required which gather information concerning the outsourced data.

5.5.3.4 *Enforcing data protection requirements*

Additionally the *CloudInspector* is also suitable for controlling the cloud provider. As Art. 17 (2) 95/46/EC states that the controller must choose a processor which can provide sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out and that he needs to ensure compliance with these measures, the tenant could for instance use the outcomes of the TEM to check what technical measures the provider carries out. Instead of just trusting that the undertaken measures do help to protect according to Art. 17 (1) and Art. 17 (3) 95/46/EC "*personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing"* the TEM enables the tenant a real inside view in ongoing internal processing mechanisms. In contrast to the "legal" solution of choosing a cloud provider which has received a certificate the TEM would therefore permit the cloud user to fulfil his duty of control. The information which the tenant receives need to be understandable even for layman. As the law is, according to Art. 17 (1) 95746/EC, imposing on the controller the appropriate technical and organizational measures "*to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing*", he is in turn legally bound to check what such measures imply. This means that he needs to inform himself about the standard of protection he needs to ensure.[160] The TEM can therefore help to check if such appropriate measures are given, especially as the physical machines are placed on the infrastructure level. With a better understanding of ongoing procedures he can also instruct the provider adequately about required actions.

5.5.3.5 *Use for Mirasys Use Case Nr. 2*

As the Mirasys Use Case Nr. 2 is focused on showing that there is a lack of transparency and thus of control enabling the data leak, the use of the *CloudInspector* could permit the user to get information about the implemented technical measures protecting "*personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing*", Art. 17 (1) 95/46/EC. At least undertaken internal management proceedings can help elucidate system specific ongoings, but they do not address directly the outsourced data measures. The *CloudInspector* is therefore strengthening the legal positon of the cloud user by enhancing transparency and thus real control but only in combination with the system internals. For the Mirasys Use Case Nr.2 it would thus be of importance to expand the information gathering also on outsourced data. Still the *CloudInspector* would permit to fulfil the data subject's access right. If for example the cloud user would have demanded the exact location of the machines and this would have shown for example the location of the machine in China and the contract prohibited the outsourcing of data outside Europe, the *CloudInspector* could have disclosed the breach of duty. In turn the *CloudInspector* has not been developed for preventing such events like a data leak. The *CloudInspector* permits therefore only

[160] Simitis, § 11, Rn. 58.

a continuous monitoring in real-time which can help repressively. It is thus very valuable for reconstructing events (like the data leak) and to determine infringements.

5.5.4 Summary and legal recommendations

The *CloudInspector* and *Hybris* are two very promising tools which can strengthen the legal position of the tenant by enabling him a provider-independent inside view in internal system operations, as it breaks through the lack of control and transparency. Whereas the *CloudInspector* gathers relevant information for a possible negligent behaviour and permits to deduct the cause from this, *Hybris* guarantees that transferred data are recorded in a tamper-resistant way. The *CloudInspector* can especially permit within the internal contractual relationships the tenant to take recourse on the provider for a breach of duty. Additionally it would be valuable to expand the information gathering on outsourced data by other tools and also on the other levels. This permits transparency on accesses and/or modifications of the data by non-authorized persons. For further development it might also be interesting to permit the fulfilment of other data subject's rights, especially those ones related to the outsourced data. As the proof of concept of the *CloudInspector* is very promising it shouldn't thus be an obstacle to transfer the methodology on other levels of the architectural framework.

5.6 Cloud Assurance Profile

5.6.1 Scope and Function

The cloud assurance methodology and framework described in deliverable D5.2[161] of the SECCRIT project aims at bettering the possibilities to gain an overview of security properties in cloud environments which poses a special challenge due to dynamic system changes inherent to cloud computing and possible involvement of a multiplicity of stakeholders. In order to achieve this, it had to be analysed how high level security can be measured per component and how continuous aggregation of measured information can be achieved.[162] The proposed approach includes a representation model for security properties, a framework capable of aggregating security properties across the components constituting a virtual service and a method to determine a level of assurance from the gathered information.[163]

Security relevant aspects are categorized in three security classes, namely confidentiality, integrity and availability.[164] Measurable security properties are then assigned to these classes, thus forming e.g. the class "confidentiality" consisting of several associated security properties like "strong passwords", "encryption" and so forth.

The assurance framework can then be used to ascertain an *Assurance Level* derived from these categorized security properties for the so-called "Target of Evaluation", where target of evaluation can either be a single "Component of Evaluation" within the cloud architecture or a "Group of

[161] See also Hudic, A.; Tauber, M.; Lorunser, T.; Krotsiani, M.; Spanoudakis, G.; Mauthe, A.; Weippl, E.R., "A Multi-layer and MultiTenant Cloud Assurance Evaluation Methodology," in Cloud Computing Technology and Science (CloudCom); Hudic, A.; Hecht, T.; Tauber, M.; Mauthe, A.; Elvira, S.C., "Towards Continuous Cloud Service Assurance for Critical Infrastructure IT," in Future Internet of Things and Cloud (FiCloud).
[162] D5.2, p. 5.
[163] D5.2, p. 6.
[164] D5.2, p. 18.

Evaluation" comprising two or more components of the cloud service in question.[165] So-called "Assurance Profiles" can be defined to specify details about the desired evaluation like, for example, security objectives, desired security properties, their relation and weighing for the evaluation result and so forth. The evaluation itself is then carried out by iterating through every component associated with the target of evaluation and its respective security properties, the latter then being depicted in bit masks[166] to enable further processing like horizontal and vertical aggregation[167]. Finally, an "Assurance Level" for the target of evaluation can be derived which represents the overall security of the system or service in question for each of the security classes.

The chosen approach aims at overcoming difficulties related with the ascertaining of assurance levels in cloud environments by enabling stakeholders to examine security properties across the spheres of different stakeholders, layers and components within a dynamic cloud environment. Since security is in a variety of ways relevant from a legal point of view, the relevance of cloud assurance with regard to legal aspects will be examined in the following.

5.6.1.1 *Legal aspects of assurance concerning liability / evidence law*

Guaranteeing a certain level of security is in many cases a key concern when it comes to implementing cloud services in a company's or administrations IT infrastructure. Security aspects are a fortiori essential when use of cloud services in critical infrastructures is in question and different stakeholders are involved in the provision of such services.

Certifying a certain level of security at a given point in time (e.g. once a year) or agreeing contractually on minimum security standards to be met by a provider only solves part of the problem. Especially multi-layered cloud architectures make it difficult to gain an overall view on security measures in place and possible security gaps, the latter posing an even greater threat in multi-layered cloud architectures, since overall system security may be compromised because of the weakest link in a chain of components. Hence it is important to implement possibilities allowing the stakeholders to check fulfilment of security requirements across components, architectural layers and spheres of the different stakeholders.

With regard to liability and evidence, a possibility to check security requirements following an overall approach could prove helpful in different ways.

If, for example, the critical infrastructure service provider in the SECCRIT architectural model relies on other third party providers like an IaaS-Provider contributing physical resources needed by the first, assurance of certain security levels is getting quite difficult. The critical infrastructure service provider may want to guarantee certain minimum security attributes to his customers, who may on their part be legally obliged to only choose providers fulfilling certain security requirements. Quite often, neither the end user nor the CIS-Provider acting as an intermediate instance will be able to check which security measures are in place within the systems running at other levels they both rely on for their services and in the end entrust their data to.

In case a security breach or any other incident occurs within a multi-layered cloud service, it may become difficult, or yet worse, impossible to elucidate if and how any of the involved stakeholders committed a breach of duty causal for damages suffered by any other party. Technical approaches like the cloud assurance and evaluation method granting improved possibilities to assess and assure certain security levels across various components, architectural layers and

[165] D5.2, p. 28.

[166] D5.2, p. 60.

[167] D5.2, p 27.

stakeholders may help to overcome the opaqueness inherent to cloud architectures that normally aggravate clarification of liabilities and gathering of evidence.

An important feature of the chosen approach is the possibility to gain insights on security levels without revealing technical details of underlying components, since most providers would not be willing to reveal all technical details about components and configurations in use within their systems. The user of a service, may on the one hand, anyways not be interested at all in technical details, but may on the other hand have a very strong interest in using only services which are able to guarantee a certain overall level of system security fitting the needs determined by his specific use case and ensuring compliance with legal or contractual obligations he himself is subject to.

The fact that with the chosen technical approach security relevant aspects are subdivided, measured, defined and expressed by terms like “classes”, “levels” and “profiles” makes it important to contractually agree upon the exact meaning and extent of these terms and to clarify beforehand what exactly can and will be assured to the user of a service. It should, for example, be clear to the user what security features he may expect and will be assured if he chooses “level 5” for the class “confidentiality” or “level 3” for the class “availability”. Clear definitions of what extent of security a certain class is meant to assure to the respective user could also help to clearly define the contractual obligations each of the involved parties is subject to and hence to determine in case of an incident whether these duties have actually been met or whether a breach of duty has been committed.

Especially critical infrastructure providers will require high guaranteed levels, as the constraints of security are in this domain very high settled, because of the higher position of trust. The critical infrastructure providers as users of the system will need to be clearly informed by the provider what each level can guarantee him. In turn the critical infrastructure provider will need to know what security measures are required in his domain. Ignorance would also lead to an own default, as it can be expected that the respective user knows the appropriate security measures he requires.

Monitoring security requirements periodically or on demand may furthermore help to document the fulfilment of contractual obligations.

In return, if a fault occurred, which has caused damage even though the cloud user has chosen a high level of security this could be an indication of negligence of the provider. In this case the cloud provider might have acted negligent as still a fault occurred even though, the high level guaranteed the user a secure system. The provider could in turn disprove the default by proving that the causality is not given between fault and damage. Therefore the assurance framework permits an additional indication for what happened within the system, but can in turn not give a one hundred percent guarantee that a high level automatically means that no fault will occur. It is very likely that the system is very well protected but still exemptions are always possible.

On the other hand, if the cloud user chooses a low assurance level, this might justify either a contributory negligence, if the cloud user did not inform the user properly and the user in turn missed to make inquires on appropriate security measures, or it might constitute an own default of the user himself. The contract should therefore clearly define the respective duties and the expected demands.

The provider could also use the outcomes of the Assurance framework to show for example, that the system fulfilled the expected high level, therefore the system was very likely not vulnerable. It will then be the duty of the cloud user to disprove this fact by other means.

The tool can therefore be used for SLA compliance, as possible records permit a check of chosen levels. Additionally it represents an indication for a possible default of the provider, if a high level was chosen and still a fault leading to damage occurred. For critical infrastructure providers it is recommended to choose a high level, especially when personal data need to be processed, as they require special protection. The Assurance framework is moreover also useful for providing both parties with additional possibilities to substantiate their respective case even stronger.

5.6.1.1.1 Use for Mirasys Use Case Nr.1

With the Assurance framework, CitySec could show a possible fault of TenSyS, if he has chosen a high level. Especially for an expert it could be useful to see what records the assurance framework provides for finding out the most probable cause for a fault. With the records of the Assurance framework and the indication of a very likely non-vulnerable chosen system, the expert will most probably come to the result, that a negligent behaviour was given. As the court is freely to assess all evidence, it will most probably follow the outcomes in the expert report. Therefore CitySec will lose the lawsuit against MetroSub, but will in return win the subsequent one against TenSyS.

5.6.1.2 *Legal aspects of assurance concerning data protection law*

The cloud assurance evaluation procedure itself does not process any personal data[168], thus rendering it fairly uncritical from a data protection point of view. It can, nonetheless, gain relevance with regard to data protection since assurance of overall security levels or specific security measures can prove helpful to ensure compliance with requirements data protection law imposes on anyone concerned with processing of personal data.

Part of the legal obligations originating from European legislation controllers and by contract processors are subject to is the duty to "*implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network* […]", since this is what member states are, according to Art. 17 95/46/EC, obliged to ensure in their national data protection laws.

Many of the security measures derived from this provision and according national implementation laws, are expressible by security attributes included in the assurance methodology. "*unlawful destruction*" or "*accidental loss*" correspond for example with measures comprised in the class "availability", while "*unauthorized disclosure or access* " correspond with the class "confidentiality" and "*alteration*" as mentioned in the directive corresponds with the class "*integrity*". Cloud Assurance can therefore be seen as part of the measures undertaken to ensure compliance with data protection legislation.

The fact that cloud assurance enables improved measurement of security measures across various components, architectural layers and stakeholders gains significantly relevance with regard to different roles defined in data protection laws. Art. 17 95/46/EC contains special regulations dealing with constellations where parties other than the controller are handling data on his behalf. Namely, it is stated that "*The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures*." This provision shows that handing over the data and processing outside of the direct sphere of influence of the

[168] D5.2, p. 6.

controller does not free him from his data protection responsibilities. Not only is he responsible for choosing a suitable processor, who is capable of fulfilling data protection requirements, he must furthermore ensure compliance with these measures. These duties are already quite difficult to fulfil in a simple outsourcing scenario with only one external data processor, not even to mention the additional complexity arising from multi-stakeholder cloud environments, where the cloud user might not even know which other companies are forming part of the services he relies on. Further detail on the (contractual) relation between controller and processor is given in Art. 17(3):

“*The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:*
- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.”

This provision further underlines, that the controller stays responsible to some extent, regardless of whether the actual processing is carried out by an external data processor and it shows, that the processor himself is also responsible for implementing appropriate security measures.

The Cloud Assurance methodology can help to trace the presence of appropriate security measures across the spheres of data controller, data processor and further subcontractors and the multiplicity of systems and subcomponents in use at the various stakeholders. It may thus help each stakeholder to ensure that he fulfils the data protection responsibilities he is subject to, especially those ones prescribed by law or from contractual duties the parties agreed upon.

The assurance level must in particular also pay tribute to the specific categorization of data the user wants to outsource. Special categories of data[169] call for stronger requirements than general personal data. This would indeed also require a higher level of assurance. Therefore the cloud user needs to be aware about the specific legal requirements he is subject to when he processes personal data.

5.6.1.2.1 Use for Mirasys Use Case 2

As the assurance framework permits to check the fulfilment of security requirements over several layers within composed systems, the cloud user gets real control options and can check if the appropriate technical measures are provided by the processor TenSys and the subcontractors (TelCom, and CloudCorp).

Concerning the problem, that a non-authorized person accessed the hosted data the Assurance framework does not recognize the access to the data but can provide the possibility to check the existence of security features intended to guarantee confidentiality of data (like ACL).

With the Assurance framework therefore it could have been checked that confidentiality was not given and appropriate security measures could have been implemented. In so doing the data leak possibly could have been prevented.

5.6.1.3 *Summary and legal recommendations*

Depending on the chosen level, the Assurance framework can help to indicate a negligent behaviour of the provider. It can in turn also shift the responsibility to the cloud user if he fails to choose an appropriate level. With regard to data protection law, the assurance framework permits a promising way of checking the fulfilment of security requirements across different service levels

[169] Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

within composed systems. It is therefore useful for the fulfilment of security requirements and obligations set by data protection legislation.

5.7 Interim Result

All developed RTD outputs are very promising for strengthening the legal position of the cloud user and thus the data subject. For a more complete view it would be of advantage if the TEM would also gather the information from the other RTD outputs and *Hybris* would also record them. This could ensure that in a respective lawsuit, the expert has more outcomes which he can analyse, helping him to determine the cause by different sources more sustainably. If for example the risk assessment shows a vulnerable system, the anomaly detection detects an event, a high assurance level was chosen, the cloud user specified his security demands and imposed the duty of ensuring them properly on the cloud provider and a fault occurred, there are several indications that a negligent behaviour of the provider is given. With more sources to analyse, the expert can easier determine the cause of the event and thus a possible negligent behaviour.

6 Enforcing developed technologies

As we have seen auditing technologies are very valuable. Especially the combination of all these tools is very useful as the outcomes of each tool can be compared to the outcomes of the other ones. The more tools showing significant similarities the easier it is for an expert to determine what exactly happened. However, it still remains questionable why providers should use these tools. Especially without any legal obligation the market often determines the success. Legally requesting the use of such tools by citing them within the legal framework would therefore be a direct option to enhance the use of such tools. Last but not least we therefore have to show if (and how) such tools can directly or indirectly be required by law.

6.1 Directly

Generally the law is technique neutral, as the direct implementation of technologies into the framework would prohibit the establishment of new technologies which wouldn't therefore cope anymore with the given legal requirements. The new upcoming data protection regulation effectively has set up provisions which do appoint directly technical mechanisms. In Art. 23 (data protection by design and by default) the use of data minimization and pseudonymisation is claimed. Art. 30 (Security of processing) stipulates in Section 1 that "the controller and the processor shall implement appropriate technical and organizational measures, such as (…) pseudonymisation of personal data to ensure a level of security. According to Art. 30 (1a) for assessing the appropriate level of security the risks that are presented by data processing have to be taken into account. Finally, Art. 33 stipulates data protection impact assessments. One possibility would therefore be to directly request the use of auditing mechanisms.
Within Art. 26 a section could be inserted which would foresee the use of such mechanisms in order to control the processor adequately. A possible wording could be:
As Art. 26 (2(i)):
The use of auditing mechanisms may be used as an element to demonstrate compliance with the requirements set out in paragraph 1 and 2a.
Or directly within Art. 26 (2(h))

- *Technically* ”make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits conducted by the controller.”
- “make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits conducted by the controller”. *The processor can make use of technical mechanisms, such as auditing tools, to demonstrate conformity with the requirements set out in paragraph 1 and 2a,.*
- “make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits conducted by the controller”. *The use of technical mechanisms for demonstrating compliance shall be favoured.*

Another possibility is to provide an *annex* to the data protection regulation which could directly name technical mechanisms concretizing the term “technical and organizational measures”[170]. Developed technologies within SECCRIT could then directly be listed.

6.2 Indirectly

Another possibility would be that the developed technologies become technical standards. Often regulations require companies to use technologies “conform to the state of the art”. If therefore technical norms would foresee the use of such tools and these tools would therefore become the state of the art as technical norms like for example ISO norms, CEN norms etc., they would indirectly also be legally demanded. The provider would then be forced to use such tools in order to be conformant to the state of the art. If therefore SECCRIT results become standards, they would in return also be indirectly legally required and fall under the ambit of the data protection regulations.

7 Conclusion

After describing the current legal evidence and data protection situation in Europe and in the respective demo cases countries, the technical deliverables and respectively their outcome have been legally evaluated in the light of cloud computing.

We have basically identified within the field of liability and evidence law as well as within data protection law a major lack of transparency which is critical for both law fields as it massively weakens the position of the cloud user. Achieving a sufficient degree of transparency is however indispensable in order to ensure that cloud resources used in the critical infrastructure domain are under adequate control at the various levels of a complex cloud infrastructure. We therefore analysed the developed technologies within SECCRIT and determined their usefulness and their possibility to heighten the respective position. Especially the combination of all these tools is very desirable as it permits a complete view in on going proceedings within the cloud. Enabling the cloud user with an inside view on internal management proceedings permits him to really assess possible negligent behaviour and collect proofs for a respective lawsuit. While within the current legal evidence situation he would hardly win his lawsuit, SECCRIT tools permit him a real chance to assert his claim. Enabling a direct inside view is additionally important for the fulfilment of the data subject’s rights. By now, the cloud user was not able to fulfil them properly, risking sanctions and legal proceedings. The developed technologies therefore represent a considerable contribution to heighten the weak position of the cloud user in cloud computing constellations.

[170] For example it could be written in this annex: „such as audit trails, assurance, anomaly detection, resilience, policies etc.

8 References

Almoguera, Jesus; Perete Carmen; de la Villa, Clara: Study on the conditions of claims for damages in case of infringement of EC competition rules. National report: Spain. Ashurst, 2004. http://ec.europa.eu/competition/antitrust/actionsdamages/national_reports/spain_en.pdf

Arbeitskreise Technik und Medien, Orientierungshilfe – Cloud Computing, 2014 https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

Article 29 Data Protection Working Party, 2008. WP 154, Working Document Setting up a framework for the structure of Binding Corporate Rules. *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf*

Article 29 Data Protection Working Party, 2010. WP 169, Opinion 1/2010 on the concepts of "controller" and "processor". http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

Article 29 Data Protection Working Party: European Data Protection Authorities adopt opinion on cloud computing (WP 196), Press Release of July 01, 2012. See: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20120701_wp_196_cloud_computing_en.pdf

Article 29 Data Protection Working Party: Opinion 13/2011 on Geolocation services on smart mobile devices, May 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

Aycock, John: Computer Viruses and Malware, Springer US 2006.

Balaban, Silvia; Pallas, Frank: Haftung und Beweis bei geschachtelt komponierten Cloud-Services, InTeR 2013, 193-198.

Balaban, Silvia; Pallas, Frank: Non simplificate nubes! Ein rechtlicher Blick hinter die Kulissen informatorischer Cloud-Forschung, DSRI Herbstakademie 2013, p. 325-342.

Bergmann, Lutz; Möhrle, Roland; Herb, Armin: Datenschutzrecht, Stand 45. Status: July 2012.

Bräutigam, Peter: IT-outsourcing und Cloud-Computing, Eine Darstellung aus rechtlicher, technischer, wirtschaftlicher und vertraglicher Sicht, 3. Edition, Berlin 2013.

Beucher, Klaus/Utzerath, Julia: Cybersicherheit – Nationale und international Regulierungsinitiativen folgen für die IT-Compliance und die Haftungsmaßstäbe, MMR 2013, 362-367.

Centre for European Policy Studies (CEPS): Protecting Critical Infrastructure in the EU, Brussels 2010. Available at: https://www.ceps.eu/system/files/book/2010/12/Critical%20Infrastructure%20Protection%20Final%20A4.pdf.

Damman, Ulrich; Simitis, Spiros: EG-Datenschutzrichtlinie, Baden-Baden 1997.

Deubler, Wolfgang; Klebe, Thomas; Wedde, Peter; Weichert, Thilo: Bundesdatenschutzgesetz, 4. Edition, Frankfurt 2014.

DLA piper UK LLP, Comparative Study on cloud computing contracts, Final report, 2015.

Ehmann, Eugen ; Helfrich, Marcus: EG-Datenschutzrichtlinie, Köln 1999.

ENISA (European Union Agency for Network and Information Security): Cloud Security Incident Reporting, 2013. Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/incident-reporting-for-cloud-computing.

ENISA (European Union Agency for Network and Information Security): Critical Cloud Computing, Version 1,0, 2012. Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing.

European Commission: Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. COM (92) 422 final, 18 October 1992.

European Commission: Cloud Service Level Agreement Standardisation Guidelines, Brussels 2014.

European Commission: Communication on a European Programme for Critical Infrastructure Protection, COM(2006) 768 final, 2006.

European Commission: DG ENTR/04/68 Country report Spain: Benchmarking of existing national legal e-business practices, 2006.

European Commission: Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final, 2005*.*

EuroPriSe, European Privacy Seal. Cloud Computing and European Data Protection Law, 2012.

Gola, Peter; Schomerus, Rudolf: BDSG Bundesdatenschutzgesetz 10. Auflage, Bonn 2010.

Härting, Niko: Schutz von IP-Adressen, Praxisfolgen der BVerfG-Rechtsprechung zu Onlinedurchsuchung und Vorratsdatenspeicherung, ITRB 2009, 35-39.

Heidrich, Joerg; Wegener, Christoph: Sichere Datenwolken - Cloud Computing und Datenschutz. In: MMR 2010, 803-807.

Hornung, Gerrit; Sädtler, Stephan: Europas Wolken. In: CR 2012, 638-645.

Hudic, Aleksandar; Hecht, Thomas; Tauber, Markus; Mauthe, Andreas; Elvira, S.C., "Towards Continuous Cloud Service Assurance for Critical Infrastructure IT," in Future Internet of Things and Cloud (FiCloud), vol., no., pp.175-182, 27-29 Aug. 2014 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6984192&isnumber=6984143

Hudic, Aleksandar; Tauber, Markus; Lorunser, Thomas; Krotsiani, Maria; Spanoudakis, George; Mauthe, Andreas; Weippl, E.R.: "A Multi-layer and Multi-Tenant Cloud Assurance Evaluation Methodology," in Cloud Computing Technology and Science (CloudCom), 2014 IEEE, vol., no., pp.386-393, 15-18 Dec. 2014 *http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7037693&isnumber=7036227*

Hustinx, Peter: Data Protection and Cloud Computing under EU law. In: Third European Cyber Security Awareness Day, BSA, European Parliament, April 13, 2010.

International Working Group on Data Protection in Telecommunications: *Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" – (*51st meeting, 23-24 April 2012, Sopot (Poland)), Berlin, Germany*.* Available at: http://www.datenschutz-erlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf?1335513083

Karger, Michael; Sarre, Frank: Wird Cloud Computing zu neuen juristischen Herausforderungen führen? Inside the Cloud – Neue Herausforderungen für das Informationsrecht. Tagungsband zur DSRI Herbstakademie 2009, S. 427-439.

Kazemi, Robert; Leopold, Andreas: Datenschutzrecht in der anwaltlichen Beratung, Deutscher AnwaltVerlag 2011.

Kilian, Wolfgang; Heussen, Benno: Computerhandbuch, 26. Edition, München 2008.

Laukannen, Sakari: The Law of Evidence in the Finnish Judicial System. In The Law of Evidence in the European Union, Utrecht 2004.

Leupold, Andreas/Glossner-Stögmüller, Silke: Münchener Anwaltshandbuch IT-Recht, part 5 Internationale Bezüge des IT-Rechts einschließlich Internationales Privatrecht, 2. edition 2011.

Lotmar, Philipp: Der Arbeitsvertrag nach dem Privatrecht des deutschen Reiches, Leipzig 1902.

Münchener Kommentar: Band 1, 7. Auflage 2015.

Niemann, Fabian; Hennrich, Thorsten: Kontrollen in den Wolken. In: CR 2010, 686-692.

Palandt, Otto: Bürgerliches Gesetzbuch, 74. Edition, München 2015.

Pearson, Siani, Privacy, Security and Trust in Cloud Computing. In Privacy, Springer, London 2013, pp 3-42.

Pohle, Jan; Ammann, Thorsten: Über den Wolken…- Chancen und Risiken des Cloud Computing, CR 2009, 273-278.

Ristenpart, Thomas; Tromer Eran; Shacham, Hovav; Savage, Stefan: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. Proceeding CCS'09 Proceedings of the 16th ACM conference on Computer and communications security pages, 199-212.

Roßnagel, Alexander, Scholz, Philip: Datenschutz durch Anonymität und Pseudonymität: Rechtsfolgen der Verwendung anonymer und pseudonymer Daten. In: MMR 2001, 721-731.

Schulz, Carsten; Rosenkranz, Timo: Cloud Computing – Bedarfsorientierte Nutzng von IT-Ressourcen, ITRB 2009, 232-236.

Schuster, Fabian; Reichl, Wolfgang: Cloud Computing & SaaS: Was sind die wirklich neuen Fragen ? die eigentlichen Unterschiede zu Outsourcing, ASP Co. Liegen im Datenschutz und der TK-Anbindung. In: CR 2010, 38-43.

Simitis, Spiros: BDSG, 7. ed, Frankfurt 2011.

Söbbing, Thomas: Cloud und Grid Computing: IT-Strategien der Zukunft rechtlich betrachtet. In: MMR 2008, XII-XIV.

Sorainen Law Offices: DG ENTR/04/68 Country report Finland, Benchmarking of existing national legal e-business practices, 2006

Thalhofer, Thomas: Grenzenlos: Compliance beim Cloud Computing. In: CCZ 2011, 222-225.

Tinnefeld, Marie- Theres: Einführung in das Datenschutzrecht, 5. edition, München Oldenburg 2012.

Weichert, Thilo: Cloud Computing und Datenschutz. In: DuD 2010, 679-687.

Wicker, *Magda*: Vertragstypologische Einordnung von Cloud-Computing-Verträgen –Rechtliche Lösungen bei auftretenden Mängeln. In: MMR 2012, 783-788.

Wulf, Hans Markus: Serververträge und Haftung für Serverausfälle: Eine Analyse der vertragstypologischen Einordnung und des Haftungsumfangs. In: CR 2004, 43-48.

Zalesinska, Anna: Civil contracts in Finnish legal systems with special consideration of electronic contracts. In: Studia Erasmiana Wratislaviensia Acta Studentium, M. Sadowski, P. Szymaniec, E. Bojek (red.), Wrocław, 2009 r., 261-275