SEcure Cloud computing for CRitical Infrastructure IT

Contract No 312758

Deliverable D.2.2

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	Legal fundamentals	
Creator	KIT-legal	
Editor	Silvia Balaban, Frank Pallas	
Description	This document contains the most relevant legal fundamentals for the project as outlined in the DoW (data protection and fundamentals of evidence)	
Creation date	02/05/2013	
Version number	2.0	
Version date	27.06.2013	
Last modified by	Kit legal	
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 ☒ Coordinator 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	10/06/2013	

Versions			
Version	**Date**	**Change**	**Comment/Editor**
0.1	02.05.2013	Initial version	S. Balaban, F. Pallas
0.4	13.05.2013	Data protection added	S. Balaban, F. Pallas
0.5	24.05.2013	Evidence law added	S. Balaban, F. Pallas
0.6	31.05.2013	Intro etc, smoothing	L. Langer, M. Tauber
0.7	07.06.2013	Review	S. Balaban, F. Pallas
0.9	20.06.2013	Review	Ioannis Chochliouros
1.0	25.06.2013	Review Integration	S. Balaban, F. Pallas
1.1	26.06.2013	Review	J. Horneber
2.0	27.06.2013	Review integr. + Finaliz.	S. Balaban, F.Pallas

Abstract

This document outlines the most relevant legal fundamentals for the project SECCRIT – prepared for an audience with mainly scientific and technical focus. In particular, these fundamentals consist of:

- fundamental deliberations on cloud-specific aspects and challenges in matters of evidence law
- and of an introduction to European data protection legislation relevant to the project's subject.

While the latter is of crucial relevance with regard to the general legitimacy of the practical application of the technologies developed in the project and must therefore be thoroughly considered from the very beginning of technology development ("Privacy and Data Protection by Design"), the former is highly necessary in matters of SLA-enforcement and liability questions and, through these, for the general applicability of cloud computing without significant legal uncertainty. The considerations included herein thus provide highly valuable input for developing secure cloud technologies that are actually applicable in practice.

The document is intended to be used as guidance by technical SECCRIT partners to investigate how the issues they address relate to any legal aspects.

Table of Contents

Table of Sections with direct technical Relevance

In order to allow the technical partners to quickly identify those sections that are most relevant to them in their doing without having to read through the legal rationales and justifications for this relevance, a list of those sections that have the most direct technical relevance is provided in the following. This is, however, primarily done to ease reading and understanding for technical partners and shall not mean that other sections are not relevant. Depending on the concrete case, all other sections not listed here might very well gain significant relevance, too.

1 Introduction

The integrated consideration of relevant legal issues from the very beginning is an integral aspect within the project SECCRIT (Grant Agreement No.312758), funded by the European Commission.

Only with solid examination of these SECCRIT-relevant legal aspects it can be avoided that the technologies developed within the full scope of the project lack essential compliance requirements and can therefore not be used in practice. Instead, a close inspection of at least the most relevant legal aspects from the very beginning of technology development ensures that no such essential requirements is overseen and that the technologies developed within the project "reflect" – *at least in a quite satisfactory scope* – these legal concepts and principles.

In the end, the constant consideration of techno-legal aspects thereby significantly enhances the practical relevance of the technologies developed within the project.

From a legal point of view, the concept of cloud computing raises numerous questions of which the most important ones stem from the fields of "evidence law" and "data protection law". Of these two, "evidence law" especially focuses on the disclosing of the disputed measures and the proving of their authenticity and integrity during, for instance, a liability conflict or a dispute over SLA-compliance. "Data protection law", in turn, is rather focused on minimizing the amount of data, recognizable or known by others in order to protect the data subject fundamental rights. For the project SECCRIT, it will thus be a core challenge to bring these two strands in line with each other by means of advanced but still practical technological concepts. In order to lay the necessary groundwork for further activities within the overall project, the deliverable at hand shall thus outline the most fundamental legal aspects of "evidence law" and "data protection law" to which the core concepts of cloud computing are of particular relevance.

In matters of "evidence law", this necessarily includes the elementary characterization of potential problems alongside the material law, explaining general contract and liability situations emerging from typical applications of cloud computing. Closely related to these issues is then the question how a certain failure or non-failure can be proven within a liability-related dispute. Liability and evidence law are therefore closely related with each other and define, for instance, who has to prove what in case of a civil conflict being brought to court. This, in turn, has significant impact on the "digital evidence" needed by the different parties, thereby also leading to specific requirements having to be met by the technologies that are to be developed in the project SECCRIT. These aspects are covered in chapter 2.

Concerning "data protection law", different legal frameworks have to be considered in the light of the specific concept of cloud computing. In order to achieve international validity of the elaborations made herein, the main focus will hereby be on Europe-wide regulations. In particular, this is the data protection directive of 1995 which has been transformed into national law across the EU. Furthermore, we will also consider the novel European data protection regulation, which is currently in the state of preparation for enactment and will presumably become effective during the lifetime of the project SECCRIT. Finally, we will also discuss the current existence of national deviations from the EU-wide directive in brief, based on the example of the German national data protection law. All these elaborations can be found in chapter 3.

As mentioned above, all these considerations will be made with a clear focus on the specifics of cloud computing instead of giving just general overviews about the respective fields of law

2 Evidence Law

In the first part of this document, which shall lay out the legal fundamentals relevant for the project, we will concentrate on the legal area that is usually attributed to the term of “evidence law”. As we will see later, the deliberations that are made in the following are of crucial importance in a multitude of regards and have significant impact on the practicability of cloud computing. Without the very fundamentals of evidence law being considered during the whole process of technology development, there is a considerable risk that elementary problems of liability, contract enforcement, or verification of obligations will not be addressed at all, or only considered at the end of the process, thus potentially requiring the technological developments to be revised afterwards. With these fundamentals being clear from the very beginning, in turn, technologies can be developed in a way that ensures such requirements to be fulfillable. Thereby, technologies of cloud computing are rendered applicable under certain circumstances in the first place. For this reason, we will lay out the fundamentals of evidence law in the following.

As there is, however, no European unified civil law, the fundamental outlines of the national (German) law shall serve as a basis in order to delineate the most important evidence and liability status quos, which can actually be generalized, so that to provide essential feedback and/or guidelines for any “alike” considerations – or approaches – under the wider scope of the EU Law. Even if the same problems, from a legal point of view, might be solved differently in other European countries, they are basically appearing everywhere in identical form. The assessment of the fundamental basics is thus done on a comparably abstract level in the meaning of rather general and therefore transferable statements.

In so doing, the fundamental terms that will be used in the following parts are:

- **Obligor:**
  A person who is legally or contractually obliged to perform an obligation.
- **Obligee:**
  The person to whom the obligation is owed.
- **Breach of duty:**
  Failure of performing the owed obligation.
- **Default:**
  The intended or negligent act or omission which leads to a breach of duty.
- **Damage:**
  Detriment which a person sustains by certain cause on his lawfully protected goods.
- **Burden of proof:**
  The responsibility for a party to prove or disprove a disputed fact.
- **Burden of producing evidence:**
  The burden of producing sufficient evidence at trial.

Based on these essential definitions, we can now go into the basic fundamentals of evidence law.

2.1 Fundamentals

First of all, it is highly important to distinguish the material and the process-side of a case: Whenever a damage occurs, the next question is effectively who can be made liable for that damage. This question represents the material side of private law. When the person is identified and it comes to a process, then the injured party does, however, not automatically receive his compensation. Instead, this depends on

the proofs he can provide and, in the cases of a non-liquet-situation[1], on the burden of proof. Such questions are part of the process-side of civil law. In the first part of the deliverable the respective basics will be delineated.

2.1.1 Material side

The material side is oriented on listing up the possible claims and identifying those that will be successful in a process. Only then does it make sense to analyze the process side and thus the actual requirements for providing digital evidence to the different parties being involved in usual applications of cloud computing. Evidence Law and liability are thus closely connected to each other as evidence law takes effect whenever liability issues come up. Therefore, deliberations on evidence law are necessary in order to concretize the enforcement of the resulting claims. In particular, this helps to disclose the dispute-setting factors which speak in favor for the liability or not. In this respect, it first has to be clarified when the liability is given at all.

For the contractual liability firstly a contract is needed, while afterwards a breach of duty must have been committed for which the obligor is furthermore responsible.

In civil law, liability therefore depends on the concluded contract. Different types of contracts have their specific regulations for liability.[2] Furthermore, in cases where no contract has been closed, tort-related regulations come into force. Those legally regulated liability rules are not equal to the lawfully based contract regulations, as the enforcement of them is more severe, especially concerning the burden of proof. Besides, there is also the possibility of an exculpation concerning third persons, who have been used to perform the obligations of the obligor. Due to the specific givens that can be assumed in the field of cloud computing and in particular for the project SECCRIT, we will focus on contractual liability in the following. In this regard, it has to be distinguished between the so-called external relationship between the obligor and the obligee (the one that is covered by the "primary contract") and the so-called internal relationship between the obligor and possible other persons (which is covered by another contract), whereas these other persons are involved in performing the obligor's duties due to the obligor's contract partner from the external contract, the obligee.

2.1.1.1 Liability: External Relationship

The external relationship describes the one between the obligor and the obligee, which is contractually regulated. Liability comes into force when a breach of duty was committed. In order to identify the relevant faults it has to be elucidated what was contractually owed by the obligor to the obligee. Furthermore after classifying the fault, the obligor must actually be liable because of that fault, which is the case when he acted intentionally or negligent. Negligence is in that context the failure to exercise reasonable care. Normally, the default is assumed but can be contradicted by the obligor if he proves the cause of the damage and shows that he isn't responsible for that cause, thereby demonstrating that he didn't act negligently or intentionally. When the cause is unclear, the obligor can exonerate himself by showing to have taken all reasonable care to ensure the avoidance of such damages.[3]

Besides, the obligor is also responsible for fault on the part of his legal representatives, and of persons he uses to perform his obligations, to the same extent as for fault he would have done himself. For the obligee it is therefore not important how many persons are used "in the background" by the obligor for the fulfilling of his duties.

[1] „it cannot be proved".
[2] This is at least the case in German Law.
[3] Palandt/Grüneberg, section 280, recital 40; BGH, decision from 14.11.1989, NJW-RR 90, 446.

In the context of a breach of duty, it is also important to distinguish between result-related and behavior-related duties. Regarding the result-related duty, the proof of fault is given when the obligations (the results) have not been fulfilled properly. The fact that a damage happened in this case already speaks in favor of a breach of duty. For behavior-related duties, the fault has to be entirely proven by the obligee. Such behavior-related duties, however, shall be excluded from further considerations, because cloud computing contracts usually induce result-related duties.

2.1.1.2 Liability: Internal Relationship

The internal relationship comprehends the one between the obligor and the other persons which the obligor uses in order to perform the demanded obligations. This internal relationship is of course also based on contracts with the obligor and the persons he uses to perform his obligations, but they are not giving the obligee a legal basis for the caused damage. The obligee can only charge his contract partner for a caused damage concerning his protected goods.[4] It is therefore important to distinguish between: a) being liable for the persons who have been used in order to fulfill the obligations of the obligor, concerning his contract partner, and; b) taking recourse on those persons being used in order to accomplish the demanded duties. While basically only the contractual partner can be the subject to a claim for damages relating to a caused harm, the obligor who had to pay the damage can very well charge in turn his contractual partner for the damage he had to pay to his client afterwards. If the person the obligor used to perform his obligations is insolvent, then the obligor would therefore be completely liable on the external side but can in return not take recourse on his contractual partner who actually committed the fault.

2.1.1.3 Liability: Causality

The question for causality is highly important for any liability question. Therefore the causality is not only relevant for contractual and tort claims but is also the precondition for the damage to actually lead to a compensation obligation. For that, there has to be a sufficient causal link between the behavior of the tortfeasor and the caused damage; highly improbable events are not implying a liability.[5] There must be a certain probability that a certain incident actually causes a kind of damage and it may not be completely unlikely that the incident leads to such kind of damages.[6] Concerning the adequacy, an objective belated prognosis has to be done while the comprehension and the foresight of the tortfeasor are not relevant. In so doing, all circumstances which could be discernible have to be considered.[7] Additionally, a duty for damage compensation is only given when the enforced damage falls under the protective purpose of the norm being drawn upon. It must be a harm which is entitled to avert such kind of damages for which the norm was enacted.[8]

2.1.1.4 Liability: Summary and Simple Example

As a result it is important to distinguish between the external and the internal side of a legal constellation typical for cloud computing. The liability is in that context always given when there is a contract basis, within which a breach of duty was committed and for which the obligor is responsible. This is particularly the case when he acted negligently or intentionally. Besides, the obligor is also

[4] Of course the tort regulation can provide him a legal basic, but contractually the charge is only possible concerning his contract partner.
[5] s. RGZ 169, 84 ff.
[6] BGH NJW 1998, 138/140; 2005, 1420; Palandt-Grüneberg, BGB, 71. edition, before section 249 recital 26
[7] Palandt/Grüneberg, aaO, recital 27 with further annotations.
[8] BGH NJW 1958, 1041; 1961, 1817; 1972, 95; 1999, 3203; 2005, 1420, contestable case-law and generalized belief; s. Palandt-Grüneberg, recital 29.

responsible for fault of persons he uses to perform his obligations to the same extent as for faults he would have done himself.

If, for example, a cleaner has the duty to clean the ground and uses dirty water which soils the floor, then the cleaner commits a breach of duty even if it was not explicitly stated in the contract that he must not use dirty water. He further on acts in that completely negligently and therefore is liable for the caused harm. The same pattern also applies to analog cases of cloud computing.

2.1.2 Process Side

When in a first step the damage has occurred, the question in the second part, the process-side, is how this damage can be proved and which party bears the burden of proof.

2.1.2.1 Burden of Proof

The burden of proof is concentrated on the material civil side and depends in particular on the chosen legal basis. Normally the obligee has to prove the breach of duty, the damage occurrence and the causal link between breach of duty and damage.[9] The obligor in contrast bears the burden of proof concerning his non-responsibility.[10] The obligee also has to prove the conditions for the compensation and the extent of that one, whereas the obligor has to prove that the cause is not lying in his "danger" zone, that he eliminated relevant risks or, respectively, sufficiently tried to do so and that the damage did thus not occur because of his fault. If this succeeds then the obligee has to unburden.[11] The obligor has in return to prove the performance of the contract, therefore he has to bear the burden of proof for the proper fulfillment of the obligations.[12] Concerning the employment of other persons, it is not important for the obligee if and how many persons are used for the fulfilling of the duty by the obligor. An exoneration is therefore not possible for the obligor.[13] Instead, the obligor has the burden of proof that the person(s) he engaged handled without fault.

2.1.2.2 Burden of Producing Evidence

Whereas the burden of proof is referring to the material side, the burden of producing evidence is in consequence oriented on the process side, as it is based on the duty of pleading certain facts. The burden of producing evidence therefore has to be taken into account, too, with particular regard to the question which party will have to declaim which fact in the process. The question is thus what facts have to be provided by the plaintiff or the defendant.

Normally the plaintiff has to expound the facts giving rise to the claim whereas the defendant is responsible for the eliminating facts. Facts which are not revealed to the court will not be taken into consideration. Once a party is in the burden of providing evidence, he will therefore have to substantiate his claim. The requirements for the substantiation are not very high at the beginning; the requirements can, however, change in dependence of the adverse party's actions and in particular when the adverse party denies the fact that should be proven.

In this case, the requirements rise gradually when the pleading is more substantiated. If it is not substantiated enough, the facts will not be considered by the court with the consequence that the claim is rejected. Once facts are substantiated, the adverse party can admit or deny them. If a fact remains

[9] S. Palandt/Heinrichs, section 280, recital 34.
[10] S. Palandt/Sprau, section 823, recital 80.
[11] Palandt/Weidenkaff, section 535, recital 19.
[12] Palandt/Bassenge, section 280, recital 35.
[13] This is only possible with regard to tort law.

unclear and unproved, the question is therefore who is in the burden of proof in so called non-liquet-situations. In that situations the decision of the court is carried out on the basis of the burden of proof ("who has to prove what?"). The decision is then made at the expense of the party that is under the obligation to furnish a proof but not able to provide this proof. If, for example, the plaintiff has to prove the fault, damage and causality and fails to provide a proof concerning the extent of the damage, then the claim can be rejected. If the defendant fails to provide the proof or the fact that he is not responsible for the caused damage, then the request should be acceded.

2.1.2.3 Accepted Proofs in Court

The party which has the burden of proof can rely on the recognized (modalities of) proofs in court which are the witness, legal inspection, instrument, interrogation of the party and the expertise evidence.

2.1.2.4 Process Side: Summary and Simple Example

Concerning the process side it is important to distinguish between the burden of proof and the burden of producing evidence. Whereas the burden of proof is important for the claim enforcement (as it is concentrated on which facts have to be proven by whom) the burden of producing evidence is concentrated on the duty of pleading certain facts. For the plaintiff, these are the facts giving rise to the claim and for the defendant those ones eliminating it. In non-liquet-situations, the proof solely arises from the (previously identified) burden of proof.

In the above-mentioned cleaning case the plaintiff would be the house owner who would have to prove that the floor was cleaned with the dirty water and that he had to pay 50 € for the re-cleaning. In response to the plaintiff having actually proven this, the cleaner on the other hand has to prove that he didn't act negligently (maybe by trying to prove that the house owner gave him the bucket with the dirty water). The same pattern applies to legal disputes over the fulfillment of duties in cloud computing cases.

2.2 Evidence Law and Cloud Computing

After having laid out the very fundamentals of evidence law, these shall now be inspected with particular focus on their interrelations with the concept of cloud computing. In so doing, we will follow the same basic structure of analysis already used for explaining the general fundamentals of evidence law.

2.2.1 Material Side and Cloud Computing

For a structured analysis of cloud computing in the light of evidence law, it has firstly to be identified what type of contract is suitable for this concept, what a major fault could be, and furthermore when the cloud provider would be deemed as acting negligently.

2.2.1.1 Contract

It will have to be assessed throughout the SECCRIT project what kind of legal contract rules in the civil law would match the contract between the cloud provider and the cloud user best. For now it appears that there are different opinions in the literature regarding the classification of cloud contracts. Additionally those have to be accurately studied as there is, at least for now, no existing case-law.[14, 15] Therefore, it will have to be elicited which contracts are particularly working for Cloud Computing. In future work following these fundamental initial considerations, it will particularly have to be considered whether there is a

[14] at least not in Germany.
[15] S.a. Fritzemeyer: Die rechtliche Einordnung von IT-Verträgen und deren Folgen, NJW 2011, 2918, 2921.

possible link to the already existing case-law attributed to application-provision, access-provision, and outsourcing contracts.[16] Those approaches could also be applicable to Cloud Computing, as it might be featuring already known elements of those contracts.[17] Considering the technical aspects of cloud computing, there is indeed a lot of resemblance to those contracts, so that it should sound plausible to rely on these case-law opinions.

Effectively the cloud computing contract is basically composed of different well-known and legally established types of contracts. In particular, it features elements of lease contracts, because the provider is ceding the use of hardware for a specified period, but also has elements of service contracts. It is also discussed whether the cloud computing contract should be interpreted as a purchase contract[18], a contract to produce a work[19], or even as a safekeeping contract.[20]

A possible approach for characterizing cloud computing contracts might be to assume different contract types for different "classes" of computing services and to distinguish between SaaS, PaaS, and IaaS-related contracts, for example. For the Software-as-a-Service concept, regulations on lease contracts might provide an appropriate framework, as this concept is focused on the software use. This approach of different contract-types being assumed for different "classes" of cloud services should be evaluated further throughout the SECCRIT project. As for now, the concentration of the expertise should not go into details, as only the fundamentals have to be disclosed.

2.2.1.2 Breach of Duty / Fault

Primarily, it has to be discussed how the fault of the cloud provider could be depicted in order to constitute a liability. A breach of duty could insofar be committed either by the cloud provider himself or by persons which the cloud provider employs in order to perform his duties, as it is undoubted that the provider can be dependent on the performance of third parties. A breach of duty is therefore given when a violation of a contract-based existing duty is assumed. A breach of duty in turn can either refer to performance-related duties or just to a protection duty in the meaning of taking account of the other party's rights.[21] The performance-related duty presumes that the extent of the duty has been contractually fixed and is therefore initially clear. A breach of duty would therefore be given in case of a failure of performing the contractually owed obligation. This could for now be imagined when the Cloud user cannot use the Cloud system or cannot relocate his data to the server of the cloud provider.[22] For this failure different reasons seem to be a possible starting point, which will have to be discussed in more detail in later deliverables. In particular, these possible reasons include breakdown, virus attacks, hacker attacks, overload and force majeure risk, which will be analyzed henceforth.

[16] Schuster/Reichl, Cloud Computing & SaaS: Was sind die wirklich neuen Fragen?, CR 2010, 38, 38.
[17] Grützner/Jakob, Compliance von A-Z, 1.edition 2010.
[18] Wicker, Vertragstypologische Einordnung von Cloud-Computing-Verträgen –Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783, 784.
[19] Wicker, Vertragstypologische Einordnung von Cloud-Computing-Verträgen –Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783, 785.
[20] Koch, ITRB 2001, 42.
[21] That means that every actor has to take care of the rights of his contract partner, like not destroying objects, even if this care-taking is not explicit part of the contract. For example, if A has to clean the house of B and while doing so drops B's flower vase, A is liable for this destruction even if no respective terms can be found in the contract.
[22] It is for sure that it has to be clear how long the failure has to be in order to classify it as a breach of duty. On the one hand it seems plausible that attendance measures sometimes require unavailability of service – on the other hand the cloud provider can switch on other servers, so the attendance of one server can oblige the cloud provider to implement redundancy measures and outsource the data on another server.

2.2.1.3 Default

A breach of duty does not automatically lead to the liability of the party having committed it. As already outlined above, it is essential for a civil damage compensation that this party is also responsible for that. This is the case when the party would have acted either intentionally or negligently. Negligence would surely be recognized when the cloud provider has not met established minimum security standards which have enabled the damage, as the interest of the cloud user lies in the maintaining of a properly functioning server.

Insofar it will have to be evaluated throughout the SECCRIT project time what else would also count as negligent behavior. By now, it seems valuable to analyze the already identified reasons for a failure (which basically is, as outlined above, a breach of duty) in more detail regarding the question whether they can actually constitute a liability.

2.2.1.3.1 Breakdown

If a breakdown leads to the outcome that data could not be stored or a service not provided, the question is whether this damage actually has to be compensated. The requirement for this damage is that the cloud provider is responsible for the data not being stored or the service not being provided. In this regard, it has to be assessed which duty of protecting the cloud provider shall be responsible for.

This depends on the general national contract regulations. If cloud computing is considered as a leasing agreement then the cloud provider would be the lessor which would have the duty to grant the lessee the use of the leased property for the lease period.[23] For this the protection against perturbs of the use of the leased object by actions and omissions and also the defense of disruption have to be assumed by the lessor.[24] The provider would therefore be legally obligated to accomplish his duty of avoiding the lack of saving data or providing a service due to breakdowns. For that it would be important that the data center being used is protected from power blackouts and secured through continuous technical attendance. Even if technical innovations are released, the provider has insofar the obligation of striking all financially reasonable measures for the improvement of the used technical devices.[25] Besides this, the provider has to keep the technical infrastructure with the state-of-the-art-technology and apply relevant technical innovation on a regular basis.[26] Therefore the provider is responsible for the duty of precaution at its best. This will, however, have to be checked attentively.

2.2.1.3.2 Virus Attacks

Generally speaking, system failures are often caused by virus attacks. In the field of cloud computing, viruses do, however, at least today play no role because their usual mode of operation does not apply to the internal mechanisms currently used in cloud computing. Viruses always require that they (or, respectively, their malicious routines) are executed to in order to actually exert their harming functionality. On end-user systems, this is regularly the case when files with active content (e.g. a word processing file including malicious scripts) are opened or when websites containing active content (e.g. scripts, flash) are called and the active content is executed automatically. The system that is in such cases harmed by the virus then is the system where the malicious code was executed. Such code-execution from files etc. containing active content does, however, usually not happen on cloud computing systems

[23] Palandt/Weidenkaff, section 535, recital 14.
[24] Palandt/Weidenkaff, section 535, recital 14.
[25] Kinne/Schach/Bieber, Miet- und Mietprozessrecht, 6. edition 2011, section 535, recital 79.
[26] Hoeren/Sieber/Komarnicki, part 12, recital 10.

themselves.[27] Another imaginable way for cloud systems to be infected by viruses is based on so-called "buffer overflows" caused by malicious data uploaded to a cloud system, causing the cloud-system's processing routines to crash and execute content that should not be executable. This attack method can, however, easily be addressed with modern technologies like "no execution" and therefore play a minor role even in the desktop-world today and, at least today, no role with regard to cloud systems. Of course, it can never be excluded that novel methods allowing viruses to successfully attack cloud systems are developed in the future, but for the moment, the relevance of viruses as a possible reason for cloud system failure seems to be considerably low. This does, however, not refer to possible questions regarding the onward distribution of virus-infected files to others. These are discussed in section 2.2.1.4 below.

2.2.1.3.3 Hacker Attacks

Different from virus attacks, hacker attacks are a considerable threat in the field of cloud computing. This becomes particularly relevant in cases where the cloud user has an own obligation for preventing such outsider attacks. In these cases, the cloud user has an interest in the respective countermeasures (including firewalls, intrusion detection systems, etc.) being in place and appropriately configured. If he wants the cloud provider to ensure this, it seems that he should close corresponding extra payable clauses for that.[28] A measure that seems reasonable for the cloud provider without explicit clauses, however, is the closing of software-bugs within the software offered to his customers – a requirement that not only applies to SaaS-offers but also to the software for realizing an IaaS, for example.[29] Which mechanisms are actually necessary without explicit contracts being closed will have to be determined in more detail throughout the project time. In any case, the provider must use sufficiently strong authentication mechanisms to protect the server against unauthorized persons. If he fails to implement those procedures, this would even be recognized as a gross negligence.

2.2.1.3.4 Overload

Concerning the problem of a service not being delivered for reasons of overload, a default would be automatically given because one of the main characterizations of cloud computing – and thus one of the main reasons for using cloud services – lies in the possibility of falling back to other servers using virtualization technologies (concept of elasticity). In the case of overload situations nonetheless happening, this strongly speaks for the cloud provider not having fulfilled fundamental duties.

2.2.1.3.5 Force Majeure

A liability because of force majeure risks is practically not imaginable. When it comes to a failure of a server due to the weather (because of a tornado or a flood having destroyed the whole datacenter, for example) the cloud provider can hardly be made responsible. This could indeed only be the case when the cloud provider had the opportunity (and probably assured his customer to actually do so in the contract) to ensure geo-redundancy by holding fallback systems with replicated data available in other datacenters located in other cities or countries but failed to actually prepare for such a handover. Anyhow there is surely going to be a regulation in the general terms and conditions (GTC) whether the cloud provider does have to make a back-up of the data or not or whether this is an additional cost-accounting performance

[27] Nonetheless, there is at least a theoretical possibility for such code-execution to happen in SaaS-environments, for example. Here, however, usual mechanisms of strong separation between SaaS-environment and the actual cloud system etc. can prevent viruses and similar software from affecting the cloud system itself.
[28] Hoeren/Sieber/Komarnicki, part 12, recital 63.
[29] Wulf, Serververträge und Haftung für Serverausfälle: Eine Analyse der vertragstypologischen Einordnung und des Haftungsumfangs, CR 2004, 43, 48.

individually agreed upon. The absence of such a regulation will indeed lead to an exculpation which would therefore not count as negligence.

2.2.1.3.6 Failure Reasons and Responsibility – Summary

In summary, the cloud provider has to ensure a secure platform. He should be easily capable of doing this because he can rely on a numerous quantity resources. The cloud provider would therefore have to implement the technical means for ensuring security in order to prohibit external attacks. Additionally, the employees of the cloud provider have to be adequately trained for being able to ensure the necessary security means to be appropriately set up and configured. Furthermore, the cloud provider must have mechanisms (especially for data replication and migration) in place in order to prevent data from being lost in case of a real failure and for preventing overload situations. Ensuring integrity and availability of data in the cloud is part of the cloud provider's basic obligations.

2.2.1.4 Contributory Negligence

It will also have to be considered if sometimes the cloud user could also be partially responsible in the meaning of a contributory negligence. Thoughtful would therefore be a failure because of a problem regarding the internet connection. Here it is important to distinguish between connection problems being caused on the side of the cloud user and those connection problems arising on the side of the cloud. In the case of recurring short-term connection outages leading to significant damage (like, for example, an integrity loss of data), it might be discussed whether a contributory negligence might also be attributed to the cloud user, as the internet connection lies, to a certain extent, also in his sphere. In such cases, it will therefore be crucial to identify the actual location of the outage-causing malfunction.

Another interesting case arises when data are outsourced which are already contaminated by a virus, and when these data are then redistributed to other parties than the cloud user who originally outsourced the infected files. In this case a contributory negligence of the cloud provider could be stated in addition to the default of the cloud user, because he missed to use security programs which could have recognized those viruses.[30] Additionally, a contributory negligence of the cloud provider could also arise when one of his cloud users suffers a damage because of an assault from another cloud user which was only possible because of an insufficient tenant-separation being employed by the cloud provider.

2.2.1.5 Duty to Maintain Safety

Besides it will have to be considered throughout the SECCRIT project time if cloud computing does on its own entail a duty to maintain safety. This duty might result from the basic liability principle that wherever a source of danger is open for the public, the one who opened it has to ensure that he has made all necessary provisions to avoid a damage of others.[31] An IT-system is considered as dangerous when its technical functions can be used for redistributing damage-causing programs or when the systems are manipulated in order to harm third persons just by provoking a system breakdown, a deletion of their data or in order to spy out these data.[32] Whenever such a risk exists, the respective systems could be regarded as a source of danger for other systems which the cloud provider has to eliminate. In such cases,

[30] Palandt/Heinrichs, section 254, recital 74.
[31] BGH NJW-RR 2003, 1459 with more indications about other case-law-decisions.
[32] Libertus, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren MMR 2005, 507, 508; Koch, Updating von Sicherheitssoftware – Haftung und Beweislast, CR 8/2009, 485, 486.

at least applying patches for known bugs and security software should be counted as a default. In summary all technical reasonable provisions should be done by the cloud provider.[33]

2.2.1.6 Liability for Sub-Contractors

Concerning subcontracts of the cloud provider, it seems plausible that the sub-contract-partners are qualified as persons whom the obligor uses to perform his obligation with the consequence that the cloud provider must be liable (concerning the cloud user) for their fault.[34] This will indeed have to be evaluated. A possible failure of a dedicated backbone operator used for doing the replication between different data centers would therefore count as a failure of the cloud provider. Besides it will also have to be taken into account that the cloud provider can use even other cloud providers for realizing their service,[35] and therefore it can come to reciprocal recriminations. If the cloud provider is blaming the other one mutually for a caused damage, then the question will indeed be who has to be made liable for that. In the foreground then stands how the burden of proof is and who will have to bear it in the cases of non-liquet-situations.[36] This depends on "who has to prove what"-questions at the process-side.

Besides, the internal liability relations within a company also have to be kept in mind. These could, for example, arise when business secrets are disclosed to competitors after they were outsourced to a cloud provider. From the internal perspective, this could induce a liability of the manager who was responsible for the decision to store such sensitive data in the cloud and thereby caused an inappropriate risk for the company. It will therefore have to be considered which data can be allocated in order to prevent such liability problems.

2.2.1.7 Cloud Provider as Someone Who Has Been Used in Order to Perform the Obligations of the Cloud User

Furthermore the cloud user can also have closed contracts with his clients and in order to fulfill the owed obligations, he might rely on the cloud provider.[37] If, for instance, the cloud user is a privately owned security firm und wants to outsource all surveillance-data (like the recordings of video cameras) and uses a cloud storage provider for this purpose, this provider might be liable concerning his contractual partner (i.e., the client for which he is obliged to do the surveillance) if the cloud provider commits a failure. It will therefore have to be evaluated throughout the SECCRIT project if the cloud provider on the other hand has to be counted as someone who has been used in order to fulfill the obligations of the cloud user. This would have the consequence that the cloud user could be made liable for faults of the cloud provider concerning the external relationship.

Insofar this seems pretty inconvenient as the internals of the cloud system are not really transparent and therefore failures can appear by hazard without anyone to blame for it. In "traditional" cases of persons being used in order to perform the obligations of other persons, such faults can usually be traced back to human misbehavior (like a cleaner not taking enough care of the object to be cleaned). In the field of cloud computing, in turn, such human misbehavior will hardly be the main reason of failure occurring in comparable settings. It will therefore have to be analyzed what this means for cases where the cloud provider is used to perform the cloud user's obligations.

[33] Koch, Updating von Sicherheitssoftware – Haftung und Beweislast, CR 8/2009, 485, 487.
[34] 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.
[35] S. for example Dropbox with Amazon, which is using the Amazon Cloud-Service Simple Storage Service S3.
[36] It cannot be proved.
[37] S. Blaha, Rechtsfragen des Cloud Computings, 100.

2.2.1.8 SLAs

As already outlined above, the existing legal regulations for IT-contracts are not satisfying[38] – particularly with regard to cloud computing – as there are significant difficulties like initially to find a suitable type of contract already legally defined that fits the technical conditions of cloud computing best.[39] While the market for cloud computing services is still in a phase of strong growth, in the long term the market is nonetheless likely to experience consolidation in the same way as other sectors, and it may evolve towards a limited number of providers offering services to a large number of customers. Such concentration could reinforce the already existing imbalance in the cloud services market between the service providers and most of the users of their services.[40]

In a recent Consultation[41] that has been supported by the Commission, it has been identified –by the involved participants- that guidelines and checklists on model terms for contracts would be useful. The question asked of respondents was about the intended usefulness of models for the description of Service Level Agreements (SLA) or End User Agreements (EUA) existed specifically for cloud services so that certain basic terms and conditions could easily be incorporated into the contractual agreements. The need of having model contracts for SLAs and EUAs at European level was a widely shared opinion among all respondent groups. Typical statements from respondents are have proposed that "*A model SLA or EUA will help Cloud services to define the rights and responsibilities of all involved parties"* or *"standard ratified models, agreements or "sections of" should be available covering the different aspects of delivery and for different purposes/levels of cover. It can then be up to the user and provider to agree which they want/need to apply to the particular service they are procuring/providing".* Respondents to this question touched upon other issues, mainly by identifying the importance for these provisions to be simple and clear so that be easily accepted by all involved players.

Although existing EU legislation protects users of cloud services, consumers are often unaware of their relevant rights especially including the applicable law and jurisdiction in civil and commercial matters, notably when it comes to contract law questions[42]. Development of model contract terms was identified in the Commission's Consultation -mentioned in the previous paragraph- as desirable to overcome these problems. Industrial users and suppliers have called for self-regulatory agreements or standardization. For contracts with consumers and small firms European model contract terms and conditions based on an

[38] Bräutigam, SLA: In der Praxis alles klar?, CR 2004, 248, 249; Hartung/Stiemerling, CR 2011, 617, 618.

[39] Traditional IT outsourcing arrangements were typically negotiated and related to data storage, processing facilities and services defined and described in detail and up-front. Cloud computing contracts, on the other hand, essentially create a framework in which the user has access to infinitely scalable and flexible IT capabilities according to his needs. However, currently the greater flexibility of cloud computing as compared to traditional outsourcing is often counterbalanced by reduced certainty for the customer due to insufficiently specific and balanced contracts with cloud providers.

[40] While governments and big companies may have the possibility to have private clouds established according to their requirements or to negotiate the service agreements with cloud providers at equal level, small and medium organisations from the public and private sectors and individual consumers will have to accept the terms and conditions as they are laid down by the service providers for public cloud services. This asymmetry could be exploited by service providers to set conditions for their services which are to the disadvantage of the clients by limiting providers' obligations and liability and restricting clients' rights, giving providers far reaching privileges and powers, even to unilaterally change terms and conditions of service to the disadvantage of the cloud client.

[41] European Commission (2011): *Cloud Computing: Public Consultation Report (Brussels, 05.12.2011). Available at: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf*

[42] European Parliament and Council (2008). *Regulation (EC) of the European Parliament and of the Council No.593/2008 on the Law applicable to contractual obligations (Rome I), [Official Journal (OJ) L177, pp.6-16 04.07.2008]. Strasbourg, France: European Parliament and Council*.

optional contract law instrument may be needed to create transparent and fair cloud services contracts. Identifying and disseminating best practices in respect of model contract terms will accelerate the take up-of cloud computing by increasing the trust of prospective customers.[43]

One of the key actions of the common European strategy in the sector[44] is to develop model contract terms and conditions to address issues not covered by the Common European Sales Law such as: data preservation after termination of the contract, data disclosure and integrity, data location and transfer, ownership of the data or direct and indirect liability. Identifying and developing consistent solutions in the area of contract terms and conditions is a way of encouraging wide take up of cloud computing services by increasing consumer trust.

As for, such model terms do, however, not exist. This results in a lack of a fitting standard-type of contract and therefore an autonomous, individually need-oriented formulation of contract clauses is recommended. The complexity and uncertainty of the legal framework for cloud services providers means that they often use complex contracts or service level agreements with extensive disclaimers. SLAs are describing the contract-matter with regard to the performance (in the sense of availability, capacity, etc.) and they can help identify what could be a fault by means of suitable definitions. The service level agreements determine the relationship between the cloud provider and professional users. Furthermore, SLAs can be used to describe the liability risks and the compensation agreements.[45] It is therefore necessary to write down the consequences in the cases there is a deviance from agreed criteria. Depending on the side of the contract partner, it is important to list some for now already identifiable and important points which should be considered for the formulating of the SLAs:

- For the cloud user it is important that a fault is clearly defined, so there is no arguing whether a certain incident is actually a breach of duty or not.
- In that direction does also the consideration go that the liability has to be clarified. The disclaiming of the liability which is in the interest of the cloud user is normally not possible for incidents resulting from the cloud provider's intention or negligence concerning the injury to life, body or health and for gross fault for other damage or for an intentional or grossly negligent breach of duty by a legal representative of the user or a person used to perform an obligation of the user.
- When there is a clause which indicates that in the cases of a failure the compensation is dispensed, it is valuable to indicate whether the clause is a gradual performance-compensation clause or a legal consequence oriented for an agreement for warrant for defects clause, as it is important to avoid interpretation possibilities.[46] This can lead to different legal consequences as the major question is when the extinction happens. Thus is the case when the performance is rendered to the obligee. Mostly the legal consequence will more be concentrated on the contractual penalty, the reduction of price or damages. The contractual penalty can be verified by the court concerning the inappropriateness. Besides, it is important that it has to be clear if a clause is a damage or a contractual penalty clause as the relation between those two can be significantly difficult.

[43] It is expected that until the end of 2013, the Commission will develop, with the appropriate stakeholders, model terms for cloud computing service level agreements for contracts between cloud providers and professional cloud users, taking into account the developing EU acquis in this field. Once the proposed Regulation is to be adopted, the Commission will make use of the new mechanisms to provide any necessary additional guidance on the application of European data protection law in respect of cloud computing services.

[44] European Commission (2012). *MEMO-12-713: Unleashing the Potential of Cloud Computing in Europe - What is it and what does it mean for me?. (September 27, 2012).*

[45] Hartung/Stiemerling, CR 2011, 617, 618.

[46] Similarly Hartung/Stiemerling, CR 2011,617,623.

- Furthermore it has to be clarified that the damage leading to compensation is also one which is typically occurring.
- Additionally it is important that the cloud user ensures that the cloud provider periodically makes backups of his data.
- Last but not least it is never a good option to formulate too detailed clauses, as the chance of the appearance of the exactly described subject matter of the clause decreases with increasing clause detail, thereby heightening the probability of disputes having to be decided on the basis of mostly unsuitable generic legal provisions which would introduce many ambiguities when applied to cloud computing contracts.

Given these basic rules of thumb, the concrete arrangements that constitute appropriate SLAs which account for the specific givens of cloud computing and probably also refer to the technologies that are to be developed during the project will have to be discussed further at later stages of the project's progress.

2.2.2 Process Side and Cloud Computing

2.2.2.1 IT-based Proofs in Cloud Computing

Concerning the existing (modalities of) proofs already mentioned in section 2.1.2.3, it will have to be clarified which one is the most suitable for the case of cloud computing.

Perhaps it will have to be taken into account that the recognized procedural proves like witness, legal inspection, instrument, interrogation of the party and expertise evidence will not work properly as one of the major problems of cloud computing is the lack of transparency.

For now it seems that suitable proofs in a process will only be the witness proof, which is the interrogation of the person which was used by the cloud provider in order to fulfill his duties and the expertise report. Acceptance by court will surely be better achieved by an expertise from a neutral and authorized IT-expert. It sounds however quite unfeasible to have an expertise opinion on the actual facts if it is, due to the fundamental technical givens of cloud computing, more than unclear what exactly happened. Even the expertise evidence won't therefore work as a 100% truthful clarification, for what exactly happened can never be told. Furthermore, such an expertise cannot easily be given, as it will in most cases be more a supposition and cannot be based on existing facts because these facts are in most cases unknown in the context of cloud computing. In the end, none of the well-established (modalities of) proofs turns out to be appropriate in legal disputes over incidents that happened in the context of cloud computing. The witness interrogation and the expert opinion might work to a certain extent but are also far from providing satisfactory evidentiary value for delivering legal judgment with sufficient certainty.

Besides the witness and expert valuation report, it will then therefore have to be reflected whether the technology itself could be an appropriate solution for providing more reliable proofs. Generally speaking, such technical proofs are already accepted as an additional (modality of) proof in certain legal areas like in the German electronic signature act regarding the electronic declaration of intent. This will have to be clarified throughout the SECCRIT project in more detail. For now, however, it sounds highly plausible that, as there is a missing transparency, evoked by the fact that the data are somewhere non-specified in the "cloud", a systematical technical proof should possibly be taken into account and would probably help to clarify liability and evidence problems when it comes to legal disputes over incidents in the context of cloud computing. Generally speaking, technical means like trustworthy logs or other markers could be the only possible proof for a caused harm which could credibly help elucidate who is liable for the damage. A technical proof could therefore also look like a concrete technical identification mark, which can help identify the possible error sources. Furthermore, a trustworthy logging of current security updates and patches actually being applied could be a possible indication of the fact that there is no negligence

certifiable. However, there are some technical requirements that have to be met for technical proofs to be actually employable in this way. For now, we will assume these requirements to be met and discuss them in more detail in later deliverables.

In any case, it seems quite important to have such an opportunity to technically prove who can be made liable, as it seems that the existing court-proofs cannot guarantee such possibility when the location of the data as well as the actual course of events is problematical. Even an expert advice would probably not work, as he would in the lack of transparency have difficulties to effectively give concrete answers where the fault was. Beside a technical court-proof evidence, which would only be a repressive one and could therefore help clarify only on the belated process-side, also a more preventive mechanism could be imagined in the meaning of a "reminder" or a "remote audit/assessment" which helps to identify potential threats or up-coming problems like missing security updates in order to avoid the formation of a damage from the very beginning. Basically, this would indeed go into the same direction as privacy by design approaches but there the "reminder" has another objective target in the meaning of preventing security problems and not legally up-coming infractions of established Law.

Such a cloud-system with technically realized court-proof evidence could definitely become more likely to be accepted by the end-users, as the burden of proof concerning the liability could be handled much easier in case of a conflict over harming incidents. With a direct preventive proof, this acceptance could grow even more as it would probably help avoid the establishment of a damage at all. It will have to be delineated in more detail throughout the project SECCRIT how such technical proofs could be designed and whether a possible "reminder" turns out to be technically feasible. In general, however, the establishment of technical proofs appears to be highly desirable in order to reduce legal uncertainty in the field of cloud computing, to thereby raise the end users' confidence in such systems and, in the end, to make the whole societal benefits of cloud computing – which have been highlighted for years – actually happen.

In order to effectively accomplish these benefits, the mechanisms employed for providing technical proofs must, however, meet certain requirements.

2.2.2.2 Behavior of the Cloud Provider in a Process

Based on these considerations, we can now examine how a cloud provider would presumably behave in a legal dispute over a malfunction. The following considerations are based on the assumption that there is a cloud user and two cloud providers. The cloud user has a contract with one cloud provider; this first cloud provider uses the second one for furnishing the lower-level cloud platform for his higher-level cloud system.

In a process over an incident which happened in the context of cloud computing, the cloud provider would typically have to disprove the default, as he is in the obligation of furnishing a proof that he didn't act negligently or intentionally. For that a denial by pleading ignorance wouldn't work as the cloud provider does for sure have knowledge about the occurrences within his offered services. This is concerning his sphere. Pleading ignorance is only possible about facts which are not covered by his own perception. If the obligor uses persons to perform his obligations, he is then forced to undertake enquiries.[47] Besides, the one who is providing the platform can surely show what he actually did to ensure a safe and secured one (how he configures his cloud system, etc.).

It could then be imagined that the cloud provider asserts that a sub-contract-partner (so the second cloud provider) is responsible for the caused damage. This could then be considered as a simple protective

[47] Zöller/Greger, section 138, recital 16.

argument and therefore as a simple denial. If the plaintiff pleads concrete facts, such a protective argument will not be sufficient to jar the plead. The cloud provider would therefore have to prove that the other cloud provider is actually responsible. As the second cloud provider will be more likely to be used in order to perform the obligations of the primary cloud provider, the first cloud provider will automatically be responsible for faults committed by the second one, just as he would have acted himself when the second one acted intended or negligent, with the consequence that blaming the second one would be futile. The cloud provider is therefore in the obligation to furnish a proof that he or the other persons he used are not responsible for the breach of duty. He will therefore have to furnish adequate proofs. The effective proofs which are accepted in court are the witness, legal inspection, instrument, interrogation of the party and the expertise evidence. The non-responsibility will probably better be proved by showing that the cloud provider took, in accordance with the demanded state of the art, all necessary measures to have a secured platform. This can probably be furnished by legal inspection showing that, for example, all security updates have been made, etc. That will be more precisely studied below and also put in relation to the former considerations about a technical evidence which should help to clarify what actually went wrong and thus where the fault exactly occured.

2.2.2.3 Process Considerations

Another interesting process consideration is also the so-called “prima facie” of evidence which permits an easier handling of the burden of proof. This is the situation when in individual cases a typical course of events is given, which is alluding, in accordance to the experience in life, to a certain cause, and which is so usual and ordinary, that the individual circumstances of the particular case are receding in their meaning.[48]

Before considering any case-specific aspects brought up by the parties of the process, this “usual cause of a certain outcome” is then assumed first. The party against which this assumption speaks would then have to provide evidence that the assumption does not hold true for the particular case. In a concrete case, this could for instance be the assumption that a certain kind of damage “usually” results from a cloud provider insufficiently having protected his systems. In this case, the damage would then initially be attributed to the assumed insufficient protection. The cloud provider would then have to prove that he actually applied adequate security mechanisms including, for example, automatic software updates, advanced intrusion detection mechanisms etc. At least for now, it is markedly difficult for the cloud provider to give strong evidence for proving that such obligations have actually been met – the cloud user could always argue that traditional logfiles and comparable “evidence” originate from the sphere of the cloud provider and could easily be forged by him in order to provide the desired “evidence”.

Several of the technologies that are to be developed during the project SECCRIT (esp. the anomaly detection and policy enforcement from WP4 as well as the establishment of audit trails and root-cause-analysis from WP5) could prove suitable in this regard by producing technical evidence that cannot be forged by the cloud provider and can therefore better be used in legal cases to determine the actual course of events that led to a certain damage.

This, in turn, does however raise another question: If the cloud provider can use the technical proofs to provide credible evidence for having met his obligations, this (intentionally) weakens the position of the cloud user in cases where the cloud provider is actually not responsible for the adverse events being discussed. If, however, the cloud provider is responsible because he did not meet his obligations, he will hardly hand over the (for him) incriminating (but still credible) digital evidence to the cloud user. Instead, he could, for example, argue that he did not produce such credible logfiles etc. during the respective time

[48] BGH NJW 1988, 2040, 2041.

or that he did so but already deleted them. The information necessary for determining the actual course of events would thus not be available to one of the parties of the process, leading to the undesirable outcome that the cloud provider might be able to prove his non-responsibility while the cloud user cannot prove the cloud provider's wrongdoing.

Again, the technologies that are to be developed in the project might prove valuable in this regard, too. If, for instance, it can be ensured by corresponding technical implementations that the electronic evidence produced by the security mechanisms to be developed are not only unforgeable and thus deemed credible in court but that this credible evidence is also available to all parties having a legitimate interest in it and cannot be turned away by the cloud provider (non-repudiation), this might again significantly heighten legal certainty in the field of cloud computing and thereby again serve the overall goal of cloud computing being more practicable and better accepted by all relevant parties, including cloud users as well as the cloud user's clients whose data are to be stored and processed "in the cloud".

2.2.2.4 Example

After all, it seems worth to illustrate those abstract considerations by a concrete example: For that we suppose that we have a cloud user which wants to outsource his main data into the cloud. Those data are necessary for fulfilling the obligation which the cloud user owes to his clients. If there is a fault leading to the fact that the cloud user cannot accomplish this duty, he will therefore have to compensate his client on the external side, if it was a contractually owed duty. He can then take recourse on the cloud provider if the fault was in the sphere of the provider (internal side), as they have closed a contract and a breach of duty occurred for which the cloud provider has to be responsible. If the provider is relying on other providers this doesn't matter as those faults are counting just as he would have committed them himself.

If we suppose that the cloud user goes to court in order to enforce his compensation, he will have to expound all the facts giving rise to the claim. This depends on the material burden of proof. Therefore the cloud user has to prove the fault, damage and causality. If he fails to provide a proof concerning the extent of the damage, then the claim can be rejected. The cloud provider on the other hand has to prove his non-responsibility, as he has to prove the eliminating facts. For that he could "say" that he did all necessary security updates. This "saying" depends on how the cloud user firstly behaved in court, how he substantiated his claim. This substantiation can change in dependence of the opposing party's actions. As the cloud provider will have to prove the fact that he isn't responsible for the failure leading to a damage, for him it would be important to have a credible logging mechanism to show that he maintained a secure cloud with all relevant and necessary security updates in accordance to the state of the art. Helpful could in that context also be a credible technical proof (see above) in order to elucidate where the exact fault was. In the case that no proof can be furnished, the decision of the court will be carried out based on the burden of proof alone. That would mean that the failure of furnishing a proof showing that the cloud provider is not responsible would lead to the fact that the request of the cloud user should be acceded.

2.3 Cloud Computing and Evidence Law – Conclusion

Concerning the material-side, already the initial classification of the cloud computing contract seems to be quite difficult, as the legally adhered existing contract types won't probably work as intended for cloud computing. Therefore the establishment of individually formulated Service Level Agreements (SLA) seems to be quite appropriate. Basically, the attractiveness of cloud computing lies in the possible adaptation to varying needs of the cloud user at any time. It is insofar a suitable option to agree on SLAs which can be adapted and easily define the liability risks and the fault definitions. The existing lack of transparency, which would otherwise presumably lead to undesirable outcomes in case of disputes, also argues for this

approach.[49] In the end, SLAs (if used properly) allow for significantly more clearness of duties and responsibilities also in the case of legal disputes and in the end a better law enforcement.

Mostly contracts have to be negotiated with the cloud provider. The client has in that cases the choice between different performance offers, which can with increasing performance promises lead to a higher compensation when those offers are not accomplished. The liability therefore depends on what was actually owed on the basis of the respective contract. Additionally the legal basis of the liability depends on the legal fundamentals but also on the contract clauses. Of the already known contract types, it seems like the cloud contract could best be assigned to the lease contract, but this will indeed have to be investigated in more detail throughout the SECCRIT project.

Regarding the breach of duty (which is the failure of performing owed obligations), it does at least seem to be a deviance from owed obligations if a service cannot be used for an certain time. Concerning the different reasons which can lead to a failure, it appears that the cloud provider can be responsible for hacker attacks and for overloading. Therefore the cloud provider owes a technically secured platform. Additionally the Cloud Provider has to ensure that his employees are well trained in order to setup and configure the different security measures correctly and to identify up-coming technical problems and act in the reasonable time to correct them. Such duties should correspond to the contract-basic duties which concretize damage compensation. Those contract-basic performances cannot be disclaimed through general terms and conditions (GTC) but are owed by the cloud provider in any case.

Furthermore, the cloud provider could also appear in a legal dispute as someone who is used by the cloud user in order to perform the duties of that last one. The implications arising for the cloud provider from such disputes between the cloud user and another (third) party will indeed have to be examined in the next months.

Concerning the process-side, it appears that there are significant difficulties for the cloud provider in proving that security measures have actually been meet. Without a possibility for showing that, for instance, a security update has been made, the provider would either end up in a so-called “non-liquet” situation where – in the absence of provability – only the burden of proof counts, or the cloud provider would be left with evidence in the form of log-files etc., which hardly provide any advantage because they can easily be discredited as “forged” by the opposing party.[50]

Novel means for producing credible (in the meaning of unforgeable) technical evidence could, in addition to clauses in the SLAs regarding the attribution of liability risks, provide a promising possibility for avoiding such non-liquet-situations as such credible technical evidence would in the first place allow the cloud provider to prove that a security update has actually been made. As outlined above, many of the technologies that are to be developed in project SECCRIT are eligible for providing such credible technical evidence. Furthermore the same technologies could, if applied for documenting the installation of security updates patches, could be a possible indication of the fact that there is no negligence. Finally, a preventive detecting “alarm system” or a sort of “reminder”, both based on the technology of remote audits could also be a good option of using credible technical evidence in order to identify an upcoming possible damage. It will surely have to be determined throughout the project SECCRIT how mechanisms based on SECCRIT-Technologies could actually work or look like in practice.

[49] Wicker, Vertragstypologische Einordnung von Cloud-Computing-Verträgen –Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783, 787.

[50] This also applies when simple log-files are time-stamped and digitally signed by the cloud provider, because even in this case, the time-stamped and digitally signed content could easily be forged.

In any case, we can constitute significant problems from the field of evidence law to be currently present with regard to cloud computing because of the fundamental properties of this new computing paradigm. These evidence-related problems have significant impact on liability questions and will expectably lead to undesirable outcomes, given that the current status quo remains as is. Based on the technologies that are to be developed in the project SECCRIT, this could be altered through the introduction of credible technical evidence and accompanying mechanisms for granting access to this evidence. In the end, this would lower the currently existing legal uncertainties and thereby heighten the practical feasibility of cloud computing in general.

3 Data Protection Law and Cloud Computing

After having laid out the fundamentals of cloud-related evidence law the next chapter will concentrate on the legal fundamentals of data protection law and their specific impact on cloud computing. As explicitly recognized by the European Union[51], the development and broader use of cloud computing raises new challenges in terms of privacy and protection of personal data.[52] Therefore, it is essential to promote measures for the clarification of the capacities of the different actors within usual settings of cloud computing in order to better allocate the corresponding legal responsibilities and to ensure that data subjects know where their data are stored, who has access to their data, who decides on the use to which the personal data will be put, etc. The level of data protection in a cloud computing environment must not be inferior to that required in any other data processing context. Cloud computing practices can only be developed and applied legally if they guarantee that this level of data protection is respected. Following to these requirements, there was a request imposed to the European Commission so that the latter to take due account of data protection issues related to cloud computing and to ensure that data protection rules apply to all interested parties.

As outlined above, this chapter is devoted to a detailed legal analysis of the legal questions in data protection law arising from explicit features of cloud computing. In particular, these questions shall be discussed from the perspective of European legislation, accompanied by a brief look onto national specifics.

Before going into the actual deliberations, some fundamental terms from the field of data protection legislation are introduced first in order to provide a common idea of legally relevant terms. On this basis, the fundamental data protection principles are then introduced and will in a further step be legally examined with regard to their impact on cloud computing. The legal assessment will be made on the basis of already existing European law as well as on the basis of foreseeable amendments for the future. Furthermore, the deliberations will be exemplified on the basis of the national German law in order to demonstrate the existence of national specifics in the implementation of European Law into national Law.

[51] See the Official Journal (OJ) of the European Union, C 33 EE, volume 56, *February 05, 2013*. In particular, consider the part referring to: *Personal Data Protection in the European Union (P7_TA(2011)0323); European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)).*

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

3.1 Fundamental Terms of Data Protection Law

With specific regard to cloud computing, some legal terms are of particular importance and shall be defined for the scope of this document. In this respect, in accordance with the definitions given in Art. 2 of the directive 95/46/EC[53] and Art. 4 Data Protection Regulation Draft. These definitions are:

- **data subject** shall mean an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, 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
- **controller** shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law
- **processing** shall mean 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;
- **processor** shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller
- **recipient** shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients
- **consent** shall mean any freely given specific and informed indication of the wishes of the data subject by which the data subject signifies his agreement to personal data relating to him being processed
- **supervisory authority** shall mean a public authority which is established by a Member State in accordance with Article 46 Data Protection Regulation draft

3.2 General Principles of Data Protection Law

Data Protection Law is based on some generic principles which apply in general to the handling of personal data. In the following, the evaluation is carried out on the basis of these principles, as only these ensure the legal assessment to be complete. The analysis orients itself at the existence of personal data (which is necessary for data protection law to actually apply at all) and based on that on the legitimacy, the purpose-boundedness, the necessity/proportionality, data minimization, data security and transparency as well as user rights and control as the generic main principles of the European data protection legislation.[54]

3.2.1 Personal Data

On the top of these principles stands the essential term of “personal data” which is defined in Art. 2 lit a of the European directive 95/46/EC as

[53] European Parliament and Council (1995): *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal (OJ) No.L281, 23.11.1995, pp.31-50). European Parliament & Council: Luxembourg.*

[54] Bizer, Sieben goldene Regeln des Datenschutzes, DuD 2007, 350ff.

> "any information relating to an identified or identifiable natural person (data subject), where an identifiable person is anyone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

In a very simple way, this means that data are considered as personal data when the possibility of linking the information to a specific person is given. On the other hand if the data is anonymized especially when large amounts of data are collected, the chance of identifying is so unlikely that the data is therefore not covered anymore by the term of personal data and consequently does not fall under data protection legislation. In addition, when data are pseudonymized it is in particular importance to make a difference between those persons being able to resolve the pseudonym because they have assigned it and all others for which it still remains a real pseudonym because they cannot reveal the identity. In the former case the pseudonymized data are still considered as personal data because the identification is possible while in the latter case the data protection law is not applicable.[55] Other opinions are saying that the legal consequence of non-applying data protection regulations like it is considered for the anonymous data is not counting for pseudonymized data and that this has to be taken into account only within the balance of interest, as the data subject does not deserve as much protection in that cases.[56]

3.2.2 Legitimacy

Data protection Law is fundamentally based on the principle of legitimacy which states that the collecting and processing of personal data is only permitted when a legitimation exists. The legitimation can result, as mentioned in Art. 7 95/46/EC, in particular from an explicit consent or a legal obligation. If neither the individual consent of the data subject nor another kind of legal authorization exists, there is a lack of legitimation and consequently, the collecting and processing of personal data is illegitimate. Concerning the consent, it is necessary that the capacity of discernment in the consequences of the decision is given.

3.2.3 Purpose-Boundedness

Art. 6 para. 1 lit. b of the European directive 95/46/EG mentions that data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. This implies that the data subject must have knowledge of the collecting and processing of the data and understand their implications. Therefore personal data may only be used for the purpose they have been collected for, in order to prevent that the data subject is unaware of the collecting of his data. Furthermore, once the data are collected for a specific purpose they cannot be reused or reprocessed for another purpose which is not covered by the basic initial purpose. The changing of the purpose leads to the need for another renewed legitimating.

3.2.4 Necessity/Proportionality

Even in case a legitimation exists, personal data may only be collected if actually necessary for attaining a specific purpose, too. This necessity is in particular declined when the same purpose can also be achieved without the collecting, processing and use of the personal data. Collection, processing and use of personal data is only legitimate when there is no other possibility to fulfill the purpose and when there is no

[55] Roßnagel/Scholz, Datenschutz durch Anonymität und Pseudonymität: Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2001, 721, 725.
[56] Bizer/Simmitis, section 3, recital 217; Eckhardt/Kramer, EU-DSGVO- Diskussionspunkte aus der Praxis, DuD 2013, 287, 288.

alternative which could affect the personal rights of the data subjects less. In this case, the collection is the only way to accomplish the purpose.

Closely related to the principle of necessity is the principle of proportionality. This is mostly the case when there is an encroachment on the fundamental rights and in particular on the right to informational self-determination. Insofar the necessity and the proportionality concur with each other. A procedure is necessary and proportionate if there is no milder possibility which is adequate enough in order to reach the focused purpose. For actually deciding whether this is the case or not, an assessment has to be made in each respective case in order to decide which of the interests to be considered deserves the superior valuation.

3.2.5 Data Minimization

The principle of data minimization focuses, as opposed to the principle of necessity, on the technical design requirements of data processing systems. While the principle of necessity circumscribes the legal requirements regarding the extent of the processing, the scope of the data minimization principle is to collect, process or use minimal personal data. It is therefore important from the very beginning to work toward a system design and a selection of data processing systems that lead to only minimum amounts of personal data being collected, processed or used.

It is, however, important to note that the principle of data minimization does not apply to any data but only to personal data as already defined above. In particular, the principle does not apply to data that is not considered personal data (anymore). This, in turn, leads to a strong call for making use of pseudonymization and anonymization techniques, as these significantly reduce the amount of data that is to be considered personal (see above). In summary the scope of the data minimization principle is to limit the risk of encroachment on fundamental rights. Privacy-enhancing technologies based on anonymization and pseudonymization play an important role in this regard.[57]

3.2.6 Transparency

The principle of transparency indicates that it has to be apparent for the data subject for what purpose a collecting and processing of personal data takes place. Art. 10, 11 and 12 of the data protection directive 95/46/EC make sure that the data subject has a right for information and for access to the respective data. The data subject should get the opportunity to decide wherever s/he wants to reveal those data to the controller or not. Furthermore the data subject needs the information about the extent of the storage and processing of the data in order to exercise his rights and more specific how to block and erase personal data. In a very simplified way, transparency thus means that what is happening with the collected, processed or used data has to be disclosed to the data subject upon her/his request.

Transparency is a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data. It is therefore essential that individuals are well and clearly informed, in a transparent way, by data controllers about how and by whom their data are collected and processed, for what reasons, for how long and what their rights are if they want to access, rectify or delete their data. Basic elements of transparency are the requirements that the information must be easily accessible and easy to understand, and that clear and plain language is used.

[57] See, for example, the context for Privacy-Enhanced Technologies (PETs) as discussed in: International Telecommunivation Union – Telecommunications Standardization Sector (ITU-T) (2012): *Privacy in Cloud Computing- ITU-T Technology Watch Report, March 2012*. Geneva, Switzerland: ITU.

3.2.7 Data Security

The guarantee of data security is regulated in Art. 17 of the data protection directive 95/46/EC. In particular, the data controller ensures the implementation of appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access.

3.2.8 User Rights and Supervision

As already mentioned above the data subject has not only a right to access but also a right to correction, deletion and blocking of his data. Besides, this guarantees him that some sort of control is exerted over the data controller. Specific regulations with regard to the control are given within national law, relying on internal data protection officers (self-control) as well as on supervisory authorities.

3.3 Cloud Computing and Data Protection Principles

Based on the above brief overview of well-established generic data protection principles, it shall now be assessed how cloud computing has to be seen in the light of these principles. In so doing, we will first present some more elaborate considerations on the current regulatory framework (section 3.3.1) and on the law that is to be applied (section 3.3.2) as well as on the problems that arise from the legal concept of "processing on behalf of the controller" which will be relevant for cloud computing (section 3.3.3). Only then are the above-mentioned principles and their application to cloud computing discussed in more detail.

3.3.1 Cloud Computing and the Current Regulatory Framework

The current legal framework regarding data protection basically rests upon the EU directive 95/46/EC which originates from 1995. This directive is not directly applicable[58] but must rather be implemented into national law by the EU's member states. However, there is currently a European Data Protection Regulation Draft under discussion which would take effect from the day of his legal validation. At this juncture, it is important to point out the difference between a directive and a regulation: While the directive needs to be implemented into national law[59] and is thus not legally binding by itself, a regulation is directly applicable.

Due to the rapid technical change which the directive from 1995 couldn't cope with anymore[60], the European Commission proposed a new legal framework for the protection of personal data on January 25, 2012. [61,62] With this regulation, the Commission aimed at a more coherent and consequent regulation for

[58] Only when it's not implemented into national Law, and it's not depending on a condition.
[59] If a Member State fails to implement the provisions defined in the directive within the given time limits this will lead to sanctions.
[60] Wybitul/Rauer, EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz, ZD 4/2012, 160, 160.
[61] European Commission (2012): *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [COM(2012) 11 final, 25.01.2012].* Brussels, Belgium: European Commission. (*http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*).
[62] European Commission (2012). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – "Safeguarding privacy in a Connected World – A European data Protection framework for the 21st Century" [COM(2012) 9 final, 25.01.2012].* Brussels, Belgium: European Commission. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF).

the European Union,[63] precisely based on Art. 16 TFEU which guarantees each person the right of protecting his own personal data. The proposed Regulation constitutes a general basis for the future development of cloud computing. Moreover, with Article 16(2) TFEU, the Lisbon Treaty introduced a specific legal basis for the adoption of rules on the protection of personal data. For that it was necessary to determine consistent data protection standards and to ensure that these standards actually become valid in all member state at once. As Member States could previously adopt more restrictive or weaker regulations which were still in accordance with the regulations of the directive, it seemed to be more effective to impose common regulations for all Member States which they cannot differ from, see Art. 288 TFEU.[64] In consequence, the amended European data protection framework will be made in the form of a directly applicable regulation and will thus automatically become valid in each Member State the day it comes into force. National Data Protection Laws will from then lose on their warranty regarding the subject matter of the regulation.

This means that currently, the applicable law is ultimately defined in the national regulations of the member states but oriented on the European directive because this had to be implemented into national law. In the future, the replacement of the directive will lead to the automatic adoption of there-defined standards while national regulations will be outdated when the Data Protection Regulation comes into force. In addition, the proposed Regulation provides an updated framework for data protection that takes into account technological developments, while at the same time remaining technologically neutral. For these reasons, it is appropriate within the project SECCRIT to basically concentrate on the European framework first and to exemplarily analyze how this is implemented nationally based on the example of the German federal Law. In so doing, the focus of this chapter will clearly be laid on those provisions that specifically apply to cloud computing.

In the following, we will therefore analyze each of the principles in the light of three different legal frameworks: After some initial considerations on the general interrelations between the principle and the concept of cloud computing, we will first concentrate on the givens of the data protection directive with regard to the respective principle and the implications for the field of cloud computing. Then it will be laid out what principle-specific implications the forthcoming general data protection regulation[65], which is intended to replace the existing directive once it will be approved, will presumably have in the same regard. Finally, it will exemplarily be laid out what implications can emerge from specific national implementations of the data protection directive.

Before going into the principle-specific considerations, we must, however, briefly clarify which legal givens are actually to be applied in the case of the collection, processing and use of personal data taking place in or being distributed over multiple European countries.

3.3.2 Applicable Law

Under the current legal framework, the identification of applicable law has to be based upon the Art. 4 95/46/EC which indicates that the data protection law of the member state where the personal data have been collected and processed is to be applied, if the controller[66] has an establishment in that member

[63] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF
[64] The direct applicability of a Regulation in accordance with Article 288 TFEU can reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market.
[65] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html
[66] Fort he fundamental legal definitions of terms like controller, processor, etc. see section 3.1 above. For more cloud-specific considerations, see also section 3.3.3 below.

state. This emanates from the territoriality principle,[67] as the controller is obliged to fulfill every data protection law of all the countries in which he has an establishment. Due to this territoriality principle, it often turns out to be highly problematic to identify the actually applicable law in the field of cloud computing, because even the cloud provider can often not determine exactly where certain data are stored or processed at a given time.[68] This leads to significant legal problems, when the data can be dislocated because the general place of jurisdiction can be changed at any time and with it the applicable law. There is, however, also an opinion which says that the territoriality principle should be given up in order to apply the law of a certain member state to those cases where the provider is addressing his service to the user in that particular member state.[69] When the cloud provider is for example addressing his services directly at German customers, then the applicable law would (according to this alternative opinion) be German law. Besides other arguments, it especially argues for this determination of applicable law that the user should be confident that the handling of his data always complies with those national regulations that s/he is familiar with.[70] There is, however, a clear gap when both the provider and its equipment (data centres, servers, etc.) are located outside the EU but the service is used by EU citizens, as is the case for example with EU citizens using the collaboration services of Box.com or Basecamp. In this case, a cloud provider would "not be caught by EU law", as the EDPS pointed out.[71] The remedy would have to be to extend the applicability of the law to such a situation, though enforcement and redress may be an issue.

Regarding the determination of applicable law for a certain act of collection, processing and use of personal data within the EU, the directive provides the following[72] different alternatives: In the case that the controller has an establishment within the member state where the collection, processing or use is taking place, the data protection law of that member state is to be applied. In the case that the controller does not have a national establishment in the member state where the collection, processing or use is carried out but has such an establishment within another member state, the data protection law of the establishment's country comes into force. If the controller has no establishment within the European union at all, in turn, the data protection law of the member state where the collection, processing and use is conducted comes into force, except when it is only used for the purpose of transit.[73] Applicable law in the field of data protection is therefore presently always national law.

It can, however, not align with the objectives of the project SECCRIT to delineate the national data protection law of any single European country within a report on the legal fundamentals of cloud computing. Instead, all assessments shall in the following be made from the European perspective – and thus, on the primary basis of European legislation – first. Only then shall it be clarified how national regulations work and what potentially may result from such national regulations, which we exemplarily do on the basis of German data protection law.

[67] Damman/Simitis, Art. 4, recital 2.
[68] Nägele/Jacobs, Rechtsfragen des Cloud Computing, ZUM 2010, 281, 289.
[69] Jotzo, MMR 2009, 232, 234; Nägele/Jacobs,Rechtsfragen des Cloud Computing, ZUM 2010, 281, 290.
[70] S.a. ; Leupold/Glossner-Stögmüller, Münchener Anwaltshandbuch IT-Recht, Teil 5 Internationale Bezüge des IT-Rechts einschließlich Internationales Privatrecht, 2. Auflage 2011, Recital 349.
[71] According To the EDPS: (i) "A cloud provider established in the EU - or acting as processor for a controller established in the EU - will in principle be "caught" by EU law; (ii) A cloud provider which uses equipment (such as servers) in an EU Member State - or acting as processor for a controller using such equipment - will also be caught; (iii) A cloud provider in other cases - even if it mainly and mostly targets European citizens - would not be "caught" by EU law".
[72] Actually, there is also a further option in art. 4 lit. b. This is, however focused on diplomatic missions, which is saying that exceptionally the law of the country of the diplomatic mission is applicable.
[73] See art. 4 lit. c of the data protection directive.

3.3.3 Clarifications on the Concept of "Processing on Behalf of the Controller"

Before examining the above-mentioned regulations, we must first explain a fundamental concept of data protection law – the concept of "processing on behalf of the controller" – in more detail. As we will see later, this concept is of crucial importance for assessing the concept of cloud computing in matters of data protection law. Basically, this concept provides certain privileges as compared to alternative legal figures for subsuming cloud computing.

"Processing on behalf of the controller" means that the processor and the controller are basically considered as one unit by data protection law with the consequence that only the controller has to assure the compliance with the data protection regulations. The processor therefore does not need a specific legitimation and is not in the responsibility of fulfilling the obligations which emerge when personal data are processed. In particular, this refers to the above-mentioned obligations like the accomplishment of informing, deleting, correcting, blocking etc. – in short: all rights which the data subject enjoys. Even if the processor therefore is "processing" the data in the meaning of recording or storing them, he is not directly obligated to act in compliance with the data protection regulations. Instead, he is only obliged to execute the instructions given by the controller whereas the controller has the obligation to control him. Therefore, the "processing on behalf of the controller" implies that the disclosure of personal data to another person is not counting as a real processing when the processor is acting for the purpose of the controller. Unquestionably, this concept provides a real benefit for both, the processor as well as the controller, over the default rules that would otherwise have to be applied. This (undesirable) alternative would be the "transfer" of personal data with the consequence that a consent or a balancing of interest is needed. Both will be explained in more detail below.

3.3.3.1 European Legislation – Data Protection Directive

At this point the concept of processing on behalf of the controller will be legally explained in the context of the European data protection directive by especially taking account of the specifics of cloud computing.

For that it is necessary to make a difference between cloud users who transfer their own personal data into the cloud and those ones who actually allocate personal data from others like for example a list of customers. While in the first example no relevant data protection problems are occurring, the second one is indeed implying this. Regarding that latter case, the 95/46/EC directive is recognizing a "processing on behalf of the controller". This contractual relationship leads to the fact that the controller (which is, in that case, the cloud user) still remains the only one who is responsible for the fulfilling of the data protection regulations. In particular, he must ensure that the processor he has chosen can provide sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out and he must ensure compliance with those measures, Art. 17(2) 95/46/EC. In this context, the controller remains the responsible person as already explained above and cannot evade from that by simply allocating the data processing to a cloud provider.

In contrast to the controller, the processor has no direct legal obligations with regard to data protection.[74] The presence of appropriate protections is in this case only assured by the fact that the controller has an obligation for carefully choosing and controlling the processor based on the need for fulfilling his own data protection obligations. Suggestions in that way are going into the direction of certifying the compliance of the processor with data protection regulations. But at the latest when the processor is

[74] See also Hustinx, P. (2010): *Data Protection and Cloud Computing under EU law*, Third European Cyber Security Awareness Day, BSA, European Parliament, April 13, 2010.

himself using yet another cloud provider[75], the certificates or guarantees provided by privacy seals, for example in a non-European country, are without effect, especially because the cloud user never has a real insight in the mechanism of the cloud-service which the provider is using. The problem of cloud computing consists in the fact that there are a multitude of parties which want to dismiss a possible responsibility, especially when the cloud provider is engaging other cloud providers through sub-contracts.[76]

After all, the cloud user is always determining the purpose and the extent of the data processing, so that it is appropriate to impose him the responsibility of processing the data correctly. This normally leads to the fact that the processer (the cloud provider) is in accordance to Art.17 (2) 95/46/EC processing the data on behalf of the controller (the cloud user). The processor therefore has to act in compliance with the instructions given by the controller, which typically leads to the consequence that he himself indirectly has to comply with existing data protection regulations too, as the controller will presumably oblige him to act correctly.[77] This usual perception of the cloud provider being merely a processor in matters of Art. 17 (2) 95/46/EC seems, however, questionable, as this requires that the controller (the cloud user) must ensure compliance with the provisions of data protection legislation (including technical and organizational security measures, for example) what he often cannot do because he has not much influence on the cloud provider.

Given that cloud computing must achieve an adequate data protection level and that cloud computing should not be hindered by regulatory conditions that don't reflect the state of the art, it can be discussed whether the cloud provider should be directly obligated to fulfill legal data protection rules. For now this is only handled by the warranty of the controller who has no significant power over the processor in matters of monitoring as well as enforcing that legal obligations are actually fulfilled. In contrast to this, direct obligations having to be fulfilled by the controller would presumably increase the actual compliance with legal obligations, thereby also leading to a heightened confidence in cloud computing. While the actual liability in the internal relationship between controller and processor has to be regulated by the contract and will see a provision that the provider has to compensate for caused damage, this is indeed affecting the private law and is not a data protection question.

On the one hand the cloud user is accepting the inherent risk of losing control over data when he relocates them and therefore he has to ensure compliance of the taken measurements, but besides that, he has no or only very limited influence in the concrete handling of the data, while the actual control can only be exerted by and in the sphere of the cloud provider. Only the cloud provider has the ultimate knowledge where the data actually reside.[78] Alone with this possession of the data, the cloud provider carries out significant influence over them and, in particular, the actual conditions of their processing and use.

While all this argues for transferring legal obligations from the cloud user to the cloud provider, it might very well be put into question whether it is sufficient to simply provide the data subject with (yet) another

[75] For example, the prominent cloud-storage service DropBox does not maintain massive own storage systems but mainly uses Amazon's Simple Storage Service S3 in the background.

[76] See also Schröder/Haag, Stellungnahme der Art. 29-Datenschutzgruppe zum Cloud Computing, ZD 11/2012, 495, 496.

[77] Furthermore and in contrast to the usual interpretation of a cloud provider being merely a processor, the Art. 29 working party highlights that in individual cases the cloud provider can also be the controller, especially when he has an own interest which overlaps the one for fulfilling the contractual obligations. See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf p. 8.

[78] Basically sometimes even the cloud provider does not really know where exactly the data are stored – but in general he "should" know it.

responsible party even if that one is not his real contractual partner. For that it is important to keep in mind that there could be an encroachment on fundamental laws like the "right for informational self-determination" known in Germany, for example. If the possibility of an infraction of such fundamental rights is given, this suggests that the data subject should get a second person which he can hold accountable because the second person is processing the data which falls under Art. 2 b 95/46/EC.

The legal consequence of infracting data protection regulations is therefore regulated in Art. 23 95/46/EC: A person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation from the controller for the damage suffered. That means that only the controller could be taken into account as the processor is acting on behalf of him and therefore both are considered as one unit. Consequently it seems quite embarrassing that the processor could act unlawfully, as the only control is effectuated by the controller, although this could lead to an encroachment on fundamental rights of the data subject.[79] In principle there is no real difference between relocating personal data to a server space by oneself or by involving someone else. The distinctive feature of cloud computing does in both cases lie in the fact that the provider could have access to the data. It could then very well be argued that this fact should also lead to a different legal evaluation with the processor also having to fulfill data protection obligations and being liable in case of these obligations not being met. This depends on the question whether "access to data" can be equated with the knowledge that these data are of personal nature. Were this the case, he could possibly be obliged to act lawfully, even though the concept of acting on behalf of the controller, which is for now to be applied to cloud computing, does not force him to do so.

A practical application of these considerations would, in turn, presumably require that the cloud user informs the cloud provider of his intention to outsource personal data. On the other hand, it could also be argued that the cloud provider, at least in those cases where he has access to the data (and possible objections about him actually performing this access notwithstanding), is also aware of the fact that the data are personal data. It is therefore important to make a difference between the (civil) contract rules, which cannot be a legal basis for the damage compensation to a third person not involved in the contract-relationship, and the compliance with data protection law, where it could be a real option to obligate the cloud provider to ensure the regulations directly, particularly taking into account that the data subject's fundamental rights are to be protected. This general notion has to be investigated in more detail throughout the project.

3.3.3.2 European Legislation – General Data Protection Regulation

For now it seems also valuable to light up how the concept of processing data on behalf of the controller will possibly be implemented in the upcoming General Data Protection Regulation.

Art. 26 (1) of the Data Protection Draft describes the procedure of processing data on behalf of the controller. The controller shall provide sufficient guarantees that appropriate technical and organizational measures and procedures are implemented where the processing is carried out. These have to be implemented in a way that ensures that the processing will meet the requirements of the regulation and that the rights of the data subject are adequately protected. Basically the same problems which have been described in the previous section arise here too because there are no differences to the former regulations.

[79] Of course the cloud provider will be contractually (so concerning the civil law) obliged to act securely but he is not legally forced to do it, (concerning the data protection law). Penalty clauses have for that to be established.

A major revision has, however, been proposed with the introduction of specific regulations for the so-called "joint controllership" in Art. 24 which could indeed go into the direction suggested above:

> "Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, pursuant to Art. 24, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them."

The idea behind this proposition is to distribute the responsibility. According to Art. 24 of the Data Protection Draft the reason for that lies in the fact that the controller is determining the purpose jointly with others, and so those others also have in particular a say in "decision-making" and – correspondingly – an influence in the concrete processing of the data. This is basically not coherent with the rather passive role model of "processing on behalf of the controller" that is assumed in many cases of cloud computing.

Consequently, there is a regulation missing which would take the "processor" into responsibility even when he is not involved in the determination of "purposes, conditions and means of the processing of personal data" only because he is possessing the data, because they reside in his domain and because the controller has no influence in the specific way the cloud computing is realized. The simple fact that the user wants to outsource data and/or processes should not impose him the total responsibility while the cloud provider makes the ultimate decisions over, for example, the exact location of the data. Instead, it is important to put the focus on the data subject, who has to be protected and therefore has to receive the major protection possibility. This can hardly occur with certification or the surveillance of the cloud provider by the cloud user, because he has not the real possibility to undertake it. It should thus be considered to put the cloud provider himself under the data protection regulation in a way so that he has to ensure a lawful processing and use of the personal data because he is in possession of these data and can easily transfer them into different countries. Under such conditions, a real ensuring of compliance cannot be granted by the cloud user and it can also not be desirable that the data subject is suffering from a lack of actually protective regulations when it comes down to the use of cloud computing with its cross-border potentials.

3.3.3.3 National Law – The German Example

At this point it seems valuable to assess the implementation of the EU-Directive 95/46/EC into national law based on the example of the German Data Protection Law (BDSG: Federal German Data Protection Act).

Section 11 BDSG describes the requirements for collecting, processing or using personal data on behalf of others. Section 11 (1) BDSG clarifies that the controller shall be responsible for compliance with the provisions of the Act, and that in particular any compensation has to be provided by him. Therefore it is necessary to fulfill the requests of section 11 (2) BDSG, which consist in choosing the processor carefully, with special attention to the suitability of the technical and organizational measures applied by him. Therefore section 11 (2) BDSG prescribes the minimal content of the contract conditions, exemplary the controller's rights to monitor the processor and the processor's corresponding obligations to accept and cooperate in this regard (section 11 (2) No. 7 BDSG). Furthermore, the extent of the controller's authority to issue instructions to the processor (Section 11 (2) No. 9 BDSG) must be fixed. However processing on behalf of the controller is only permitted in the cases where the cloud provider is operating the service

exclusively in Germany or in another member state of the EU or a signatory state to the EEA.[80] This is often averred with Section 3 (8) BDSG.[81]

To outline the characterization of the processing on behalf of the controller, it is important to point out that firstly the controller remains the responsible person and therefore he has to fulfill the data protection regulations and secondly, the controller is liable with regard to the external side and can only claim the cloud provider (processor) internally based on the contractual relationship. If the cloud provider has negotiated an exclusion of liability then the second internal claim fails. The cloud provider is therefore not a third party within the meaning of Section 3 (8) BDSG. Thus there is no need of a consent of the data subject because it is a neutral transfer which does not need a specific legitimation as it's not considered as a processing in accordance to Section 3 (4) BDSG. Instead, the provider is a sort of an "extended arm" of the cloud user. For this result, it is, however, essential that the controller must remain the "master" of his data and the provider does indeed only collect, process or use the data as instructed by the controller, Section 11 (3) BDSG.

This can, however not be assumed in usual cloud setting, where a small or medium enterprise as the cloud user is in a significantly weaker position as opposed to a large cloud provider who is anything but reliant on this specific cloud user. For this common case, it seems therefore quite unbearable to give instruction to a large cloud provider on how to allocate and handle the data in order to ensure that data protection rules are not violated. Furthermore the control of the compliance with the technical and organizational measures as prescribed by data protection law is difficult to realize for the cloud user,[82] especially because the cloud user is usually reverting to standardized offers. Beyond that, there is also a considerable disparity of bargaining power between public[83] cloud provider and a medium-sized company, so that the medium-sized company can hardly take influence on the contractual composition.[84] Controlling the processor is in those cases not feasible, in particular because all clients of the provider would have this right. In the (hypothetical) case of an individually negotiated contract between cloud user and cloud provider, it would then be impracticable if the provider would have to justify himself towards his clients. On this basis, it seems almost idealistic to expect that the cloud user can actually get information about the present technical and organizational measures, let alone that he gets physical access to the hosting environment in order to fulfill his legal controlling obligations.

It is therefore discussed to rely on a certificate confirming the compliance with a certain security / data protection standard instead of conducting excessive explicit controls.[85] Such a proof could also be provided by an independent authority after conducting an external audit.[86] For now there are only a few cloud-specific certifications and privacy seals which exist, especially in the area of Data Protection Law. A recognized privacy seal is, for instance, the EuroCloud Star Audit SaaS privacy seal.[87] Cloud providers are additionally referring to ISO 27001 concerning the specific measures taken for information security or to SAS 70 Type 2 certificates, which were developed by the AICPA.[88] As mentioned above it seems doubtful if

[80] Schuster/Reichl, CR 2010, 38, 41.
[81] It will have to be checked if this is also the case for the European right.
[82] Possible could be a sending of a record about the realized measures, like the procedure of the activities, see Schuster/Reichl, CR 2010, 38, 42.
[83] Concerning the private cloud the appointment happens internally.
[84] Heidrich, Wegener: Sichere Datenwolken - Cloud Computing und Datenschutz, MMR 2010, 803, 806.
[85] Thalhofer, Grenzenlos: Compliance beim Cloud Computing, CCZ 2011, 222, 223; Niemann/Hennrich, Kontrollen in den Wolken, CR 10/2010, 686, 691.
[86] Weichert, DuD 2010, 679, 685; Heidrich, Wegener: Sichere Datenwolken - Cloud Computing und Datenschutz, MMR 2010, 803, 806; Niemann/Hennrich, Kontrollen in den Wolken, CR 10/2010, 686, 692.
[87] Giebichenstein/Weiss, DuD 2011, 333ff; Hennrich, Compliance in Clouds, CR 8/2011, 546, 552.
[88] American Institute of Certified Public Accountants.

certification or privacy seals are effectively an option when it comes down to the cross-border use of cloud computing.

The question to what extent such certificates provide a (legally) viable option for ensuring the compliance with data protection rules will also be evaluated in more detail throughout the project.

3.3.3.4 "Processing on Behalf of the Controller" – Summary and Implications

In summary it will have to be considered if the processing on behalf of the controller is a real option for Cloud Computing. The fact that the cloud user has to control the cloud provider and furthermore to give him instructions are effectively not coping with the actual practice of cloud computing which is based on simple standard clauses. Therefore the influence of the cloud user on the cloud provider can hardly be as adequate enough as it is imagined by the legislator. Even certificates will possibly not be sufficient, when the cloud provider is falling back on other providers. Besides this, the fact that the data are transferred into the sphere of the cloud provider, where the cloud user has no influence, can easily lead to an encroachment on fundamental rights of the data subject. The focus should (legally) therefore more be put on the protection of the data subject.

For now the principles will be explained in the light of the specifics of cloud computing.

3.3.4 Personal Data and Cloud Computing

As already stated above, data protection law is only applicable when personal data is collected, processed or used in a certain case. Personal data, in turn, are according to Art. 2 lit a 95/46/EC defined as any information relating to an identified or identifiable natural person (data subject). At the beginning of any consideration of data protection aspects of cloud computing, it must therefore be asked whether such personal data are actually present.[89]

Beyond this stands the question what "personal data" could actually be when it comes down to establish cloud computing. As mentioned above, personal data are any information relating to an identified or identifiable natural person and can for example be a company's customer data, the IP-address[90] of natural persons accessing a certain cloud service and of course the content data being collected, processed and used on a certain cloud system.[91] Personal data can also be allocated or self-chosen authorization credentials even if the establishment of personal reference is not given for outsiders, as long as the cloud provider can – directly or indirectly – determine the natural person connected to these credentials.[92] If emails are stored within the cloud, any information contained in the email-account, and in particular the address book and the senders – basically have to be considered personal data.[93] In the case of a costumer-relationship-management-system personal data could be all business partner names and their contact addresses managed by that system.[94] It has, however, to be noted that information about legal persons like companies – as opposed to those about natural persons – are basically not covered by the

[89] There is an opinion which says that it is not possible to legitimately transfer personal data to the cloud in general, s. MMR-Aktuell 2010, 304963.
[90] The notion of IP-addresses being personal data by themselves is hardly contentious in legal discussions. This aspect shall, however, not be elaborated in detail by now.
[91] Splittgerber/Rockstroh, Sicher durch die Cloud navigieren – Vertragsgestaltung beim Cloud Computing, BB 2011, 2179, 2180.
[92] Simitis/Dammann, Section 3, Recital 10.
[93] Splittgerber/Rockstroh, Sicher durch die Cloud navigieren – Vertragsgestaltung beim Cloud Computing, BB 2011, 2179, 2180.
[94] Splittgerber/Rockstroh, Sicher durch die Cloud navigieren – Vertragsgestaltung beim Cloud Computing, BB 2011, 2179, 2180.

definition of "personal data".[95] Informations about such legal persons do therefore not fall under the provisions of the Data Protection Law. The same applies to anonymized data. Anonymized data are a modified version of the original data that leads to the situation where the attribution to identified or identifiable natural persons is not possible or would require disproportional input on time, cost and manpower.[96] In this regard, the replacement of the name by other (e.g. numerical) identifiers comes into consideration, but in doing so it must be in particular be ensured that identifiers cannot be resolved to actual names anymore. In particular, this requires the deletion of any mapping tables or the like used during identifier assignment, which would otherwise allow for a reversion of the identifier assignment.[97] Such anonymized data do not pose a risk for any individual's fundamental rights and are therefore excepted from the protective measures of data protection law.

Of high relevance especially for cloud computing is the question whether encrypted personal data can be assumed anonymized data in matters of data protection law. If this is the case, data protection laws would not be applicable to such encrypted data and furthermore it would also permit to ban authorities from accessing the data. Doing so would, however, only be a solution in the cases where the data do not have to be processed further and could therefore be encrypted before being transferred to a certain cloud system. If some sort of further processing is necessary, established encryption mechanisms cannot be used to prevent the data from having to be considered personal data, though. In these cases, the comparably new concept of Fully Homomorphic Encryption (FHE) algorithms,[98] which permit to process the data in encrypted form,[99] might gain significant relevance in the future. Besides this, the aggregation of sufficiently large amounts of personal data from different data subjects into single data points might in certain cases be used for anonymization[100] and thus for ensuring that certain data are not to be considered personal data in the legal sense, thereby allowing to "evade" data protection laws.

Beyond the possibility of making data not "personal" in the legal sense anymore, encryption mechanisms would also have the consequence that even the Cloud Provider could not access the data anymore. Given that the encryption mechanism is robust enough, that the concrete implementation actually prevents illicit access to the respective data and that the natural person cannot be easily identified by other means[101], traditional as well as the rather novel homomorphic encryption might thus very well be an integral building block for ensuring compliance with data protection laws in cloud computing. It will have to be determined throughout the SECCRIT project in more detail to what extent and under what concrete conditions and requirements such mechanisms can actually be applied.

3.3.4.1 European Legislation – Data Protection Directive

As already mentioned, the definition of personal data can be found in Art. 2 lit a 95/46/EC. However there is no definition of anonymous data in the directive. The European Commission envisaged a definition in the beginning of the creation of the directive but decided that in the data processing field the fact of a

[95] Nonetheless, there are also exceptions. In Switzerland and Austria, for example, also "personal" data from legal persons are protected.

[96] This is the explanation in the German Data Protection Law, Section 3 (6) BDSG. The concept of anonymization stands in contrast to the pseudonymization, where the identification can be resolved with less effort and so data protection law remains applicable.

[97] Simitis/Dammann, BDSG, 7. Aufl. 2011, section 3, recital 206.

[98] *Gentry*, Fully homomorphic encryption using ideal lattices, in: Proceedings of the 41st annual ACM symposium on Theory of computing, 2009, 169–178.

[99] Heidrich, Wegener: Sichere Datenwolken - Cloud Computing und Datenschutz, MMR 2010, 803, 806.

[100] Simitis/Dammann, BDSG, 7. Aufl. 2011, section 3, recital 210.

[101] Splittgerber/Rockstroh, Sicher durch die Cloud navigieren – Vertragsgestaltung beim Cloud Computing, BB 2011, 2179, 2181.

disproportionate effort is hardly given, because the attribution to a certain person can therefore easily be managed in a little while without effort.[102] However the word anonymous is emerging in recital 26, concerning the principles of protection which shall not be applied to data rendered anonymous in such a way that the data subject is no longer identifiable and concerning the codes of conduct within the meaning of Art. 27, which may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible. Beyond this, art. 6 states that personal data shouldn't be kept in a form which permits the identification of data subjects for a time longer than is necessary for the purposes for which the data were collected or for which they are further processed. This can be achieved by rendering them anonymous.[103]

3.3.4.2 European Legislation – General Data Protection Regulation

According to Art. 3 (2) of the current draft of the General Data Protection Regulation, personal data is defined as "any information relating to a data subject whereas a data subject is an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, 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." In this regard, there is thus no significant renovation in comparison to the existing regulation in the directive.

The General Data Protection Regulation is not mentioning the anonymization. It is only listed in recital 23 with the consequence that the principles of protection should not be applicable. The recital 23 is therefore using the original terms of the recital 26 of the directive. As the regulation would in comparison to the directive become valid in all European countries it seems preferable to directly have a definition of the anonymous data and to clarify the legal consequences exactly within the articles as the simple citation in recital 23 does not seem sufficient enough.[104]

Also the pseudonymization is not mentioned within the Data Protection Regulation, which should possibly be taken into account, in terms of the importance and the meaning the regulation is going to have.

3.3.4.3 National Law – The German Example

Section 3 (1) BDSG defines personal data as any information concerning the personal or material circumstances of an identified or identifiable natural person (data subject). In Section 3 (6) BDSG there is furthermore a definition of "anonymized data" whereas in Section (6a) BDSG "pseudonymized data" are defined. Anonymization means the alteration of personal data so that the information concerning personal or material circumstances cannot be attributed to an identified or identifiable natural person or that such a re-attribution would require a disproportionate amount of time, expense and effort. Pseudonymization means replacing the data subject's name and other identifying features with another identifier in order to make it impossible or extremely difficult to identify the data subject. Anonymizing in the way it is described in Section 3 (6) would lead to the fact that the BDSG is not applicable anymore as no personal data would – according to the above-mentioned definition – be in place. As already outlined above, the anonymization must however fulfill strict requirements for the existence of personal data to be actually denied. Under certain circumstances, this can especially be reached by cryptographic means (including fully homomorphic encryption) or by aggregating sufficiently large amounts of personal data.

[102] Ehmann/Helfrich, EG-Datenschutzrichtlinie, art. 2, recital 23ff.
[103] Dammann/Simitis, EG-Datenschutzrichtlinie, art. 6, recital 17.
[104] S. Eckhardt/Kramer, EU-DSGVO- Diskussionspunkte aus der Praxis, DuD 2013, 287, 288.

3.3.4.4 Personal Data and Cloud Computing – Summary and Implications

As the processing of "personal data" opens up the field for the application of data protection law, it is therefore useful to think about an anonymization mechanism which will consequently lead to the fact that the data protection law will not be applicable anymore. However it, will have to be considered how this could technically look like in order to achieve the demanded requirements for actually considering the respective data as not being person-relatable anymore and thus for negating the appliance of data protection law.

3.3.5 Legitimacy and Cloud Computing

The principle of legitimacy constitutes that, different from most other legal concepts, any collection, processing or use of personal data is illegitimate as long as it is not explicitly allowed by a legitimation for doing so. This legitimation can for instance arise from the consent of the data subject, a contractual legal obligation or the legitimate interest pursued by the controller. In the lack of a legal basis like those ones mentioned above the collection, processing and using is forbidden.

It is therefore necessary to make a difference between cloud users who allocate their own personal data into the cloud and cloud users who want to relocate data from third parties. While in the first case the basis of legitimation is a contractual one it seems complicated to provide such a basis when the data subject is a third person. Regarding the possibility of basing the legitimation on the consent of the data subject is hardly a real option because it would be necessary to receive a consent from each client of the cloud user which is nearly impossible. Without this consent, however, the processing would not be legitimate anymore. The only remaining option would then be a balancing of interests in the meaning of considering which interests are overriding – those of the cloud user or those of the data subject.

Another legitimation results from the structural model of "processing on behalf of the controller" already discussed above. This model introduces a privilege, because the cloud provider is in this case acting on the basis of the contractual obligation with his user and does therefore not need an own consent of the data subject. The only responsible person remains the controller in this model and thus the cloud user himself. Therefore the cloud user would need a consent from his client or in the lack of it a legitimate interest which outweighs the data subject's interest for fundamental rights being protected. The processing on behalf of the controllers lies between the need of a consent and the balancing of interests and is therefore a privilege because the processor is not deemed as a controller who would have to comply with data protection rules.

Nonetheless as already mentioned most of the regulations regarding the structural concept of "processing on behalf of the controller" do not fit with the characteristics of cloud computing. It will therefore have to be determined whether the privilege arising from "processing on behalf of the controller" could endure. On the one hand the processor does in this model not need a real consent from the data project, which would be impossible as he doesn't have any direct[105] knowledge about the data subject, but on the other hand the above-mentioned approach of obligating the cloud provider directly to fulfill the security requirements because of the fact that he is possessing the data would also be eligible. In the case of the cloud provider not adhering to those measures, the data subject would then get another liability person which would have to cope with the objective of data protection, thus the protection of fundamental rights

[105] It can therefore be possible to argue that the cloud provider does know the content because he possesses the data and with that also the personal data of the data subject; another opinion could be that he does know that those data are personal ones only when the cloud user has informed the cloud provider that he wants to store and process personal data. This controversy will be analyzed in later deliverables

and freedoms of natural persons, and in particular their rights to privacy in the meaning of Art. 1 95/46 EC.

In summary, the privilege arising from the concept of "processing on behalf of the controller" could indeed be useful in the field of cloud computing as the alternative option of the data subjects' individual consent is not practicable in this field. Nonetheless, it will have to be discussed whether cloud-specific amendments like a certain direct responsibility of the cloud provider seem recommendable for the future.

3.3.5.1 European Legislation – Data Protection Directive

On a European level, the principle of legitimacy is reflected in art. 7 95/46/EC, where the criteria for making data processing legitimate are specified. The only legitimations of particular relevance for cloud computing are given in Art. 7 (a) 95/46/EC, which is the consent, Art. 7 (b) 95/46/EC, which is the necessity for the performance of a contract to which the data subject is party and finally Art. 7 (f) 95/46/EC, which refers to processings that are necessary for the purposes of the legitimate interest pursued by the controller except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Art.1 (1) 95/46/EC. Whereas Art. 7 (b) 95/46/EC provides the legitimation when cloud user and cloud provider are acting on a contractual basis, the effective question is when the legitimate interest overrides the interest for fundamental rights. This is mostly a case-by-case decision which depends on the specific particularities. This will be discussed during the consideration of the national law below.

Furthermore, it is important to highlight the specific regulations for the legitimacy of transferring data to third countries. European data protection law stipulates tight controls on the processing of personal data and its transfer outside the European Economic Area (EEA). As a result Art. 25 95/46/EC in conjunction with Art. 26 are regulating the requirements for the lawfulness of such transfers. Data can only be transferred to third countries when those countries have achieved an adequate level of data protection.

This has been recognized for Switzerland, Andorra, Argentina, Australia, Canada, Faeroe Islands, Guernsey, State of Israel, the Isle of Man, New Zealand, Eastern Republic of Uruguay, Jersey and for the US concerning the Safe Harbor and Transfer of Air Passanger Name Record Data.[106] It is therefore important for the Cloud Provider to respect the adequate level of protection and for that at its best an offering of data processing and recording in the EU would be advisable. Furthermore it is possible relating to Art. 26 (2), (4) 95/46/EC that the controller submits to the Safe Harbor Regulations or the Binding Corporate Rules within the Art. 25 (1), (2) respectively Art. 26(2) 95/46/EC. The Safe Harbor Rules have been established in 2000 especially for the US. They are in accordance to the American Law and comprehend fundamentals like the information of the data subject concerning the purpose of the processing and the possibility of choosing the transmission of the data to third parties or the using of the data to other purposes and an obligation of data security. US-companies can register themselves following a self-regulatory concept, when they want to receive data from the EU. Partially this self-regulation seems insufficient because it cannot offer enough security.[107] The user must make sure that the level of protection is adequate enough. For that he has to be warrant of the information obligations and suspend a possible transmission to third persons.

3.3.5.2 European Legislation – General Data Protection Regulation

Under the proposed EU Data Protection Regulation Draft, the processing of personal data is legitimated in Art. 6 (a) when the data subject has given his consent for one or more specific purposes, in Art. 6 (b) when

[106] http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm
[107] S. Thalhofer, Grenzenlos: Compliance beim Cloud Computing, CCZ 2011, 222, 224.

it is necessary for the performance of a contract to which the data subject is party and in Art. 6 (f) when the legitimate interest override the interests or fundamental rights of the data subject. Concerning direct two-party relationships with the data subject himself being the cloud user, the alternative (b) is coming into action. In the case that data of clients are processed, the "primary" contract between the client and the cloud user cannot serve as a legitimation for the "secondary" process of outsourcing between cloud user and cloud provider. The cloud usage is unquestionably not happening in order to fulfill the obligations of the primary contract but only for easing and economizing office work and for that because of company-internal reasons alone.[108]

Concerning the possible modality of the data subject's consent, it is however indispensable to point out that this should be carried out in well-recorded form for procedural reasons as Art. 7 (1) explicitly imposes the burden of proof for the data subject's consent actually being given to the controller. Furthermore the modality of consent is excluded for providing legitimation in cases with a significant imbalance between the position of the data subject and the controller, Art. 7 (4). An indication for that could be an economic dependence, like in the case of outsourcing employee data to the cloud.

Regarding the processing outside of the European Union, the requirements for the transfer to third countries must be met. This is regulated in chapter 5 of the Draft for a General Data Protection Regulation. Firstly Art. 40 appoints that any transfer of personal data to a third country may only take place if the conditions of this regulation are complied with by the controller and the processor. This in particular refers to the adequacy of a level of protection, which is conformant to Art. 41 but also the rule of law, the judicial relief and the existence of an independent supervisory authority. Unless an exception applies, the data controller must adduce adequate safeguards for the protection of personal data: for example, enter into a contract with the recipient of the data ensuring that the data will remain adequately protected. The problem is that these rules rely on a definition of data transfer from "point-to-point" (P2P). They require having a contract, and sometimes a notification to the authority for each transfer to a country where the legal framework is not adequate. In practice this is very difficult to implement, particularly in cloud computing that entails the continuous transfer of personal data. As it happens with the question of applicable law, this challenge is not unique for cloud computing, although cloud computing makes it more acute. To this aim, the Commission will review standard contractual clauses applicable to transfer of personal data to third countries and adapting them, as needed, to cloud services; in parallel, the Commission may call upon national data protection authorities to approve Binding Corporate Rules for cloud providers.

Without an adequacy decision like the one mentioned in the Art. 41, there is a need for appropriate safeguards as stated in Art. 42, especially in form of standard data protection clauses.[109] These can also be adopted by a supervisory authority in accordance with the consistency mechanism referred to in Art. 57, but this has to be generally accepted by the Commission. For cloud computing Art. 42 could be relevant, especially when a case-by-case transfer of data is legally allowed. That could be the binding corporate rules, the standard data protection clauses and the contract clauses. Art. 43 is furthermore listing the conditions for the transmission based on binding corporate rules. Art. 44 is cataloguing the derogations for a transfer to a third country. It is legally permitted for the ensuring of a public interest and can under closely defined circumstances with a legitimate interest for the controller, when the transfer process has been verified and documented before, be justified. The commission and the supervisory authority of third countries, where the level of data protection has been recognized as adequate, can develop a mode for an international collaboration for the protection of personal data and take into consideration the recommendation of the organization for economic co-operation and development (OECD) from the

[108] Hornung/Sädtler, Europas Wolken, CR 10/2012, 638, 641.
[109] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, p. 12.

12.06.2007 concerning the cross-border collaboration in regard to the implementation of the data protection rules (cross border co-operation in the enforcement of laws protecting privacy).[110] For cloud computing, it is therefore indispensable to have an adequate level of data protection present at the place of ultimate data processing in order to make the outsourcing of personal data outside of the EU legitimate. In particular, this adequate level can also be infracted by national laws, including regulations for government access like in the US, which lower the level of protection for the data subject. It can therefore be hard to ensure such an adequate level in cases of cloud computing being performed outside of the EU.

3.3.5.3 National Law – The German Example

Besides the individual consent, the German data protection law allows for a legitimation based on the balancing of interest which is provided in section 28 (1) s. 1 no. 2 BDSG and which defines that the processing of data is legitimate as far as it is necessary to support legitimate interests of the controller and there is no reason to assume that the data subject has a more serious legitimate interest in the personal data not being processed. A legitimate interest is furthermore one which is – based on a reasonable consideration of the specific circumstances – justified as a real interest, which can also be economical or ideational.[111]

Therefore, the cloud user's interest in cost reduction and an increased competitiveness of the company infrastructure must be put in relation with the interests of the data subject, like the employee or the clients of the user, that those data are not outsourced to an unclear platform.[112] The higher the environment provided by the cloud provider is, the less do the interests of employees or clients weigh in this consideration, leading to a higher probability of the weighing of interests being made in favor of the cloud user. Even if the cloud provider is thus not directly put into the respective responsibility by data protection law, a high level of security might serve as a significant basis for legitimating the use of cloud computing by means of a balance of interests between cloud user and data subject. It is, however, important that the personal data in question are not special categories of personal data as mentioned in art. 3 (9) BDSG, because those ones are sensitive data which underlie more restrictive regulations.[113]

Basically the transfer of personal data is legitimate when it is performed to a safe platform.[114] In most cases, however, an individual decision has to be done.[115] The transfer into third countries is regulated in sections 4b and 4c and perfectly matches the givens of the current data protection directive outlined above.

3.3.5.4 Legitimacy and Cloud Computing – Summary and Implications

In summary the consent does not seem to be practicable as the legitimating ground for cloud computing, as the cloud user would need a consent from every client. In a large company with for example 500 individual persons as clients whose data is to be stored "in the cloud", this would mean that the cloud user, so the large company, would have to get the consent of every single client, which is

[110] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, S. 13.
[111] Bergmann/Möhrle/Herb, BDSG, section 28, recital 222.
[112] Leupold/Glossner-Stögmüller, Münchener Anwaltshandbuch IT-Recht, Teil 5 Internationale Bezüge des IT-Rechts einschließlich Internationales Privatrecht, 2. Auflage 2011, Recital 351.
[113] Niemann/Paul, K&R 2009, 444, 449.
[114] Anders Spies, MMR-Aktuell 2010, 298882; Leupold/Glossner-Stögmüller, Münchener Anwaltshandbuch IT-Recht, part 5 Internationale Bezüge des IT-Rechts einschließlich Internationales Privatrecht, 2. edition 2011, recital 354.
[115] S.a. Leupold/Glossner-Stögmüller, Münchener Anwaltshandbuch IT-Recht, part 5 Internationale Bezüge des IT-Rechts einschließlich Internationales Privatrecht, 2. edition 2011, recital 352.

practically not imaginable. Also the weighing of interest would require a legitimate interest of the cloud user which has to outweigh the data subject's interest for fundamental rights being protected. This is going to be a specific case-by-case-weighing, which is, however, also influenced by the security level provided in the specific cloud setting (see also section 3.3.10) . When the environment is highly secured the interest of the cloud user can therefore easier override the fundamental rights of the data subject. Last but not least in cases of the transfer of data into third countries, it should be ensured that an adequate level of data protection (comprising all fundamental principles) is guaranteed, which cannot always be taken for granted.

3.3.6 Purpose-Boundedness and Cloud Computing

According to the principle of purpose-boundedness, personal data shall be collected for specified, explicit and legitimate purposes alone and not further processed in a way incompatible with those purposes. Furthermore, once the data are collected for a specific purpose, they must not be reused or reprocessed for another purpose which is not covered by the initial basic one. Any change of the purpose requires another separate legitimation.

With regard to cloud computing, the collecting of personal data is firstly carried out by the cloud user and thus, the controller. Therefore the cloud user must collect the data for a specified purpose and can process them only in accordance with that purpose. This means that, as the cloud user is the controller, his purpose must be covered by the legal basis which allows him to process the data.[116] Controllers should therefore be deterred from using information for incompatible purposes. A controller storing medical records must, for instance, ensure that these are not used for other purposes. If he has the data subject's consent or if the balancing of interest will be in his favor then the recording and the processing are legitimate as long as they are carried out for this initial purpose. The question is, then, whether the transfer of the data to a cloud provider would constitute a change of purpose as cloud provider and cloud user (processor and controller) are considered as one single unit.

As long as the functionalities realized by means of cloud computing are the same that would otherwise be realized inhouse (on own servers, for example), this will hardly constitute a change of purpose. With regard to purpose limitation, it makes no difference whether, for instance, a customer database is maintained within a local or within a cloud-based customer-relationship-management system. The transmission, processing and use of the data are still carried out for the purpose that the cloud user had for initially collecting the personal data. This does, however, change if the transfer to a cloud-based environment is done in order to integrate it with other cloud services providing further functionalities that are not covered by the initial purpose. In this case, a new legitimation would be needed for using the data for the newly added purpose, too. In this regard, there is however no difference between cloud computing and "traditional" practices (except maybe for the fact that cloud computing offers much more possibilities for purpose-changing integrations with other services). The mere relocation from local infrastructure to a cloud provider does not constitute a change of purpose relevant to the principle of purpose-boundedness, though. The same is true for the case that the initial collection is also done by a cloud provider (processor) on behalf of the cloud user (controller). Here, the processor does not need a specific purpose and the collection is bound to the purpose as pursued by the cloud-user.

3.3.6.1 European Legislation – Data Protection Directive

As indicated above, Art. 6 (1) lit. b 95/46/EC mentions that personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Recital 28 is furthermore indicating that the processing must be lawful and fair to the

[116] See also section 3.3.4.

individuals concerned, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed. This implies that the data subject must have knowledge of the collecting and processing of the data.[117] When the data are, for instance, customer relationship data, it is also in the data subjects' interest that the company does have their personal data. The collecting and further processing is however restricted to the same purpose and may not be altered without a separate legitimation for doing so.

3.3.6.2 European Legislation – General Data Protection Regulation

Art. 5 (b) is determining that a purpose must be given for the collecting and processing of the data. Insofar the same considerations as above are also valid for the regulation draft.

3.3.6.3 National Law – The German Example

Generally speaking, the German Data protection Law provides the possibility of changing the purposes as mentioned in section 28 (2, 3) BDSG under certain conditions. Furthermore, section 31 BDSG indicates that personal data recorded exclusively for purposes of monitoring data protection, safeguarding data or ensuring proper operation of a data processing system (logging data etc.) may only be used for these purposes and may not, for instance, be reused for monitoring employees' working times. For all other cases, there is no real change in the purpose implied by the mere use of cloud computing, so these regulations are not acting restrictively.

3.3.6.4 Purpose-Boundedness and Cloud Computing – Summary and Implications

As a result the relocation from local infrastructure to a cloud provider does not constitute a change of purpose. The purpose from the original scope (for what the data have been collected) is still given when the cloud user decides to relocate them on an external server. If the manager of a company wants to have a business relationship with his client and therefore saves the client's contact data and on a later stage decides to switch to cloud computing, then the purpose, so the business relationship interest does not change. Nonetheless, it must be ensured that the migration of data and processes to the cloud may not lead to the data being used for other purposes, which may happen for example when existing data or services are integrated with other cloud services providing further functionalities that are not covered by the initial purpose. This could, for example, be the case when the cloud solution used by the manager automatically uses stored contact data for preparing targeted advertisements.

3.3.7 Necessity/Proportionality and Cloud Computing

The principle of necessity is closely related with the principle of purpose-boundedness and is focused on the fact that data should only be collected if it is actually necessary for attaining a specific purpose. This is in particular not the case when the purpose can be achieved without the collecting, processing and using of personal data. The fact of cloud computing being used implies no significant changes in this regard: If it can be assumed that the collection, processing and use of certain personal data is necessary for attaining a specific purpose, this is basically still the case if the purpose is attained with the help of cloud-based technologies.

It might, however, be discussed in more detail whether the fact of cloud computing being used implies a change in the "mildness" of the means in the sense that cloud computing is deemed "less mild" than the local collection, processing and use of the respective personal data. This could, for instance, be argued because of the possibility of third persons having access to data stored "in the cloud" and because of other risks being introduced by using cloud computing. As the principle of proportionality is concentrated

[117] Hoeren/Sieber, Multimedia-Recht, 32. edition 2012, recital 78.

on the fact that a procedure can only be legitimate if there is no milder possibility of attaining the respective purpose, such a notion would imply that local variants would always be preferable over cloud-based ones, making cloud computing illegitimate in a multitude of cases. This discussion will, however, have to be made during later stages of the project.

3.3.7.1 European Legislation – Data Protection Directive

The principle of necessity is based upon the Art. 7 95/46/EC and is also mentioned in the recital 30. Other specifics relevant for cloud computing cannot be observed within the Data Protection Directive with regard to this principle.

3.3.7.2 European Legislation – General Data Protection Regulation

Within the Data Protection Regulation Draft it's the Art. 6 and 9 which depict the principle of the necessity. Recitals 35 to 37 and 40 are also listing it. Again, no other regulations with particular relevance for cloud computing are present in the General Data Protection Regulation Draft with regard to this principle.

3.3.7.3 National Law – The German Example

In the German BDSG it is the Section 28 (1) BDSG which is citing the principle of necessity. No cloud-specific regulations can be found here, too.

3.3.7.4 Necessity/Proportionality and Cloud Computing – Summary and Implications

Finally the necessity principle does not result in significant, cloud-specific problems. If the collecting, processing and use of personal data is necessary then it makes no difference when the controller relies on a cloud provider in order to attain his purpose from a necessity perspective. If the collecting of the data for a business interest is necessary, then this also applies for the case of cloud computing being used. There might, however, be the problem of cloud-computing being deemed as "less mild" than traditional in-house computing. Discussions in this regard will have to be made later in more detail.

3.3.8 Data Minimization and Cloud Computing

The principle of data minimization indicates that personal data must be collected, processed and used in the smallest possible extent in order to limit the risk of encroachment on the data subjects' fundamental rights. It is, however, highly important to note that this constraint only applies to personal data and not to the amount of data being collected, processed and used in general. The amount of personal data, in turn, can not only be minimized by collecting, processing and using less data but also by depersonalizing personal data before they are processed and used.

Anonymization and Pseudonymization can prove highly valuable here: If personal data is anonymized before being fed into some cloud-service, these data do not represent personal data anymore. This has two implications: first, it minimizes the amount of personal data being processed and used, thereby serving the principle of data minimization, and second, the anonymized (non-personal) data within the respective service are not subject to data protection regulations.[118] This does, however, require that 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.

anonymization procedure actually prevents anyone from re-establishing the person-relatedness by whatever means (including datamining, for example).[119]

Pseudonymization, in turn, means the replacing of the data subject's identifying characteristics by another identifier in order to make it impossible or extremely difficult to re-identify the data subject for others than those who were initially intended to. This leads into a direction comparable to that of anonymization: Even if in this case the person-relatedness can be re-established by intention, pseudonymization can be employed by replacing an explicit person-relatedness (say, a name) by another unique identifier before feeding the data into a cloud-service for further processing and by re-establishing the explicit person-relatedness on the result provided by the service later. In this case, the explicit person-relatedness is not visible for the cloud provider. Even if the provider might in this case be able to re-attribute the data to a certain person (again, by means of datamining, for example), this basically also serves the goal of data minimization. Nonetheless, pseudonymized data are, differently from anonymized data, not generally considered non-personal data. The question under what circumstances (and for whom) pseudonymized data is to be deemed personal and when non-personal data does, however, depend and a multitude of specific givens and can only be answered on a case-to-case basis and should also pay attention to the question who might be able to re-attribute the data in the future. This risk of a possible future re-attribution should also be considered when choosing the concrete pseudonymization mechanism.[120]

Both, anonymization and pseudonymization are therefore of strong interest for the project as they allow for the cloud-based processing and use of data which would not be allowed to be processed and used in personal form. In particular, anonymization by means of aggregation of personal data might be of significant interest for the use-cases currently discussed. The employment of pseudonymization mechanisms, in turn, is also of interest because it is, following the principle of data minimization, compulsory whenever it is possible to attain a given purpose on the basis of pseudonymized data instead of data explicitly attributed to a given natural person. Depending on the use cases and the concrete technical approaches being pursued in the future, the possible application of anonymization and pseudonymization techniques will thus have to be considered in more detail.

3.3.8.1 European Legislation – Data Protection Directive

Recital 26 of the data protection directive is indicating that the directive is not applicable when the data are rendered anonymous in such a way that the data subjects are no longer identifiable. Consistently with the above explanations, this calls for applying at least anonymization techniques wherever possible.

3.3.8.2 European Legislation – General Data Protection Regulation

In Recital 30 of the current draft for a General Data Protection Regulation, the principle of data minimization is directly claimed with the postulation that data shall be limited to the minimum necessary for the purposes for which the data are processed. Furthermore this necessitates ensuring that the data collected are not excessive and that the period for which the data are stored is also limited to a minimum. This is also explicitly described in the Art. 5 c). Additionally the processing of personal data may only take place as long as the purposes could not be fulfilled by processing information that does not involve personal data.[121] Furthermore, Art. 23, which is accordant to the privacy by default and privacy by design

[119] Tinnefeld/Ehmann, p. 187.
[120] S. Roßnagel/Scholz, Datenschutz durch Anonymität und Pseudonymität: Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2001, 721, 731.
[121] In this regard, see also the discussion on feeding a cloud-service with pseudonymized data and re-attributing the result delivered by the service locally.

approach, also specifies that the controller shall implement mechanisms for ensuring that personal data are not collected and retained beyond the minimum necessary for the respective purposes, both in terms of the amount of personal data and the time of their storage. Again, this is completely consistent with the discussion made above.

3.3.8.3 National Law – The German Example

In the German data protection act, the principle of data minimization is reproduced in section 3 (a). The Section states that the collection, processing and use of personal data as well as the selection and design of the respective systems shall be aligned with the goal to collect, process and use as few personal data as possible. Furthermore, personal data should be rendered anonymous or pseudonymous as far as possible given the purpose for which they have been collected and/or further processed. Again, this perfectly aligns with the above-given explanations on the principle of data minimization.

3.3.8.4 Data Minimization and Cloud Computing – Summary and Implications

Anonymization and pseudonymization have to be considered as an interesting option for the SECCRIT project as the consequence of using them would surely lead to an avoidance of infracting the data subject's fundamental rights. For instance, in the case of a traffic management system based on the tracking of individual cars, it makes a significant difference whether individual car plates being recognized or not. An anonymous way of traffic analysis (based on non-identifiable representations of single cars or even on aggregations of 10 or more cars) would always be preferable from the perspective of data protection. If, however, the identification of single cars is necessary for a certain purpose (like toll-collection, for example), it would be preferable to pseudonymize the individual representations (e.g. car-plate numbers) by other identifiers before sending the data to the cloud. In any case, the concrete technical mechanisms for realizing data minimization depend on the specific case. Insofar, it will have to be determined what kinds of technical mechanisms are particularly suitable for typical scenarios of cloud computing.

3.3.9 Transparency and Cloud Computing

The principle of transparency is based on the fact that the data subject has to be informed about the collecting and processing of the personal data related to him/her in order to be able to exercise his/her rights for data protection and informational self-determination. It should therefore be apparent to the data subject that a collection or a processing of his/her personal data is taking place.

With specific regard to cloud computing, the principle of transparency however seems to be infracted and is not working properly as one of the main characteristics of cloud computing is the concept of composing cloud services from other ones without this composition being visible to the cloud user. Another problem with regard to the principle of transparency under the conditions of cloud computing arises from the maxim that the data subject should have the opportunity to be informed (by the cloud user who originally collected his/her personal data) about all locations where the data relating to him/her are transferred to. Depending on the concrete technical design, specific concepts of cloud computing can lead to the situation even cloud providers are rarely capable to indicate where (on which physical machine in which data center or even in which global region) the data are in real-time.[122] In this case, the data subject's possibilities for critically reviewing how and where his/her personal data are handled are significantly restricted.

[122] https://www.european-privacy-seal.eu/results/fact-sheets/Cloud%20Computing%20FS-201207-DE.pdf

Furthermore, it is important that the Cloud Provider is also furnishing the details about possible subcontracts. The principle of transparency therefore implies a disclosing of the significant information about such subcontracts related to the processing of personal data. Especially in multi-personal relationships where the cloud user relocates personal data from third parties to the cloud, the data subject has to be informed about all respective details. Transparency is however often lacking with respect to cloud service provider processes, procedures and practices, including whether or not cloud service providers sub-contract any of the processing and if so, what their respective processes, procedures and practices; this lack of transparency makes it difficult to conduct a proper risk assessment and also makes it more difficult to enforce rules regarding data protection.[123] This seems quite unreasonable because the relocating is only happening as part of the "primary" activities of fulfilling the contract between the cloud user and his client. In data protection law, however, the term "processing" includes the collection as well as the recording/storing. This, in turn, would result in the process of storing the data remotely at a cloud provider having to be considered as an additional and new act of processing. Even if the cloud user's collection of personal data unquestionably happened on a legitimate basis, this new process would then raise a new need for being compliant with the applicable data protection law. In question stands therefore whether the first collecting should not permit the cloud user to handle the data he wants to and to consider the storage on cloud servers only as part of the activities for performing the primary contract. Collecting should therefore also permit to relocate them later on. On the other hand the cloud user transmits the personal data to a third party and thereby discloses them.

For the principle of transparency, this implies that in multi-personal situations, the data subject has to be informed about the details of the processing by the controller.[124] This seems quite embarrassing as the cloud user would therefore be obliged to explain to each data subject (his client) why he wants to out-source the personal data of his client. This, in turn, implies that the cloud user has to be informed about the cloud provider's internal details of processing and use of the data because he is in debt of explaining this to his client. Given that there is often a lack of transparency within the handling procedures of the cloud provider, the cloud user can hardly attend this duty of transparency relating to his client. The same problem also applies to those cases where the cloud provider is acting as a processor on behalf of the controller, even if in this case the relocation of the personal data is not counting as a disclosure.[125]

Simultaneously the cloud user suffers from a loss of control over his data or the personal data of others as they are allocated in the sphere of the cloud provider.[126] In the case that the data are transferred to third countries, the possibilities for prohibiting, for example, the government's access to the data are considerably reduced. The US Patriot Act is one such example, where national interests are weighted higher than some data protection consideration.[127] Without appropriate transparency mechanisms, a data subject would have no chance of getting aware that his/her data has been transferred to locations with such adverse conditions at all. This, in turn, would massively restrict his/her data protection rights.

It is therefore indispensable to think about a solution for the effect that the cloud user cannot fulfill his duty of disclosing the details of data handling to the data subjects. In this regard, it could be an option that cloud providers are contractually bound to disclose the actual details of data handling, including the

[123] International Working Group on Data Protection in Telecommunications (2012). *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

[124] S. Gola/Schomerus, section 11, recital 4.

[125] Erbs/Kohlhaas-Ambs, Strafrechtliche Nebengesetzte, 192. edition 2012, D.7.25; Gola/Schomerus, section 11, recital 4.

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

[127] Nägele/Jacobs, Rechtsfragen des Cloud Computing, ZUM 2010, 281, 289; Spies MMR 2009, XI, XII.

location of the data as well as other relevant information.[128] The technologies that are to be developed in the project SECCRIT might prove highly valuable in this regard as, for example, information and technical mechanisms developed in the context of secure audit trails might also be used for providing information about a cloud provider's internal processes to the cloud user or even to the data subject himself/herself.

3.3.9.1 European Legislation – Data Protection Directive

In the existing Data Protection Directive, the transparency rights discussed here are represented in art. 10,11,12 95/46/EC. These make sure that the data subject has a right of information and access to it. This information right consists in disclosing the identity of the controller and of his representative, but is also listing that the purposes of the processing for which the data are intended have to be named and of course any further information such as: the recipients or categories of recipients of the data; the existence of the right of access to and the right to rectify the data concerning him. Such further information has to be furnished which is necessary to guarantee a fair processing in respect of the data subject. The data subject has also the right to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense, a confirmation as to whether or not data relating to him are being processed. In addition, information at least regarding the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, but also a communication to him in an intelligible form of the data undergoing processing and of any available information as to their source have to be provided. Important is also the fact that the data subject gets knowledge of the logic involved in any automatic processing of data concerning him. This shows that for the cloud user, this can hardly be effectuated, because he actually does not know what the cloud provider is doing.

3.3.9.2 European Legislation – General Data Protection Regulation

The title before the Art. 11 of the current draft for the general data protection regulation is dedicated to the "transparency and modalities". Art. 11 indicates that the controller shall have transparent and facile accessible policies with regard to the processing of personal data and for the exercise of data subject's transparency rights. The controller (the cloud user) should furthermore provide any information and any communication relating to the processing of personal data to the respective data subject. These efforts can hardly be made when the cloud user does not have this information at hand because the cloud provider does not provide them.

The other relevant articles based on the information necessities are art. 14 and 15. As to the principle of transparency, the question is whether smaller or medium-sized companies are able to meet the requirements laid down in art. 11 like the obligation for providing transparent and easily accessible policies. Art. 31 furthermore claims a notification to the supervisory authority in case of a breach of personal data having happened, whereas art. 32 is requesting a communication to the data subjects affected by such a data breach under certain conditions. With regard to these notification obligations, it is in particular questionable whether the given timeframe of 24h is reasonable in the case of cloud computing or, respectively, how such quick responses can be supported by the technologies developed throughout the project. At least art. 31 (1) s. 2 also permits a belated report with an additional justification.

[128] S. https://www.european-privacy-seal.eu/results/factsheets/Cloud%20Computing%20FS-201207-DE.pdf

3.3.9.3 National Law – The German Example

The regulations regarding transparency in line with the regulations from the current directive are laid out in section 4 (3) of the German federal data protection act. Insofar, no significant differences from European legislation are apparent.

3.3.9.4 Transparency and Cloud Computing – Summary and Implications

Cloud computing suffers from a lack of transparency, as the cloud user which is in the obligation of informing the data subject about what is happening to his personal data cannot fulfill this, because cloud computing is not effectuated in a matter of disclosing what is happening to the data. The cloud user therefore does not know where exactly those data are processed, and the opacity is even increased in the cases of sub-contracts. He consequently is in an embarrassing situation, if the client for example wants to get to know what is happening to his data. Therefore the technologies which will have to be developed in SECCRIT will have to pay tribute to those considerations and provide ways for allowing the data subject to comprehend the inner workings of cloud-based processes.

3.3.10 Data Security and Cloud Computing

The principle of data security obligates the controller to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. These measures have to guarantee a level of security suitable to the risks related to the processing of personal data. Cloud users are in principle bound by this obligation and must put in place "state-of-the-art" technical and organizational measures to avoid personal data from being compromised. Taking into account the state of the art and the cost of their implementation, such measures have to ensure a level of security that is appropriate to the risks emanating from the processing and the nature of the data that is to be protected. The concrete manifestation of these appropriate technical and organizational measures – that is, in particular, the decision about which measures are necessary and which ones are dispensable – is to be chosen for each case which needs to be assessed. Under the specific givens of cloud computing, it seems especially challenging for the controller to actually assure these measures to be taken. As the usage of cloud services is usually not transparent, the cloud user can hardly guarantee a certain level of security and/or a certain set of security measures to be actually taken.[129]

Currently, it is discussed that the cloud provider should assure the presence of such measures to the cloud user by means of certificates or privacy seals based on external audits.[130] Even if such certificates can prove a certain, basic set of security measures to be in place that also focus some fundamental, cloud-specific security issues arising from cloud technologies like multitenancy-architectures[131], for example, such certificates can hardly guarantee the accordance with data-protection-related security requirements arising from the very specifics of a certain use case. For example, a cloud provider might be able to prove by means of a certificate that his data centers have a certain level of physical protection against intruders, show that strong separation mechanisms between different virtual machines are installed or prove that he has a standardized process in place for the regular backup of virtual machine images etc. In a specific case with a multitude of different kinds of personal data being involved, with each kind of these data calling for specific security measures being taken because of specific data protection risks (like it is for example the case for certain categories of sensitive data), and with a multitude of involved users having

[129] AK Technik und Medien, Orientierungshilfe Cloud Computing, 2011, p. 13ff. http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf
[130] Such as EuroPriSe or EuroCloud Star Audit SaaS.
[131] Hornung/Sädtler, Europas Wolken, CR 10/2012, 638, 639.

to access the data in different roles and thus with different privileges, the presence of appropriate security measures can by nature not be ensured or even proven by means of rather generic certificates being issued for the cloud provider or his datacenters on the whole.

Instead, the question which security measures are necessary and appropriate can for large parts only be answered on the basis of the concrete case, the types of personal data involved, the ways that these personal data are interrelated with each other, the processing that is to be and could be conducted on these data and the specific risks arising for the data subjects' rights from all of this. In the traditional computing model, the responsible party could ensure (and prove) the presence of such specific security measures within his own datacenter, where he was in full control of the whole technological setting and where respective inspections were comparably easy to realize. Under the model of cloud computing, in turn, this is not true anymore. Neither is the responsible party – now the cloud user – in full control of the whole technological setting, nor can he be sure or even validate that specific security mechanisms he has taken with regard to the case-specific requirements are actually in place, configured properly and working correctly.

Many of the technologies that are to be developed during the project SECCRIT are aimed at this fundamental challenge arising from the concept of cloud computing in one way or another: The methodologies for risk-assessment, policy specification and process-oriented security guidelines from WP3, the policy decision and enforcement model from WP4, or the technologies for the establishment of audit trails and for root-cause-analysis from WP5, to name just a few, are all connected to the challenge of ensuring a case-dependent appropriate level of security in remotely used cloud settings. Besides the already mentioned problems, this might possibly also provide means for coping with the problem of personal data from the EU being transferred to and processed on cloud systems outside the EU where the presence of even fundamental security mechanisms can today not be assessed without doubt.

3.3.10.1 European Legislation – Data Protection Directive

The guarantee of data security is regulated in Art. 17 95/46/EC. According to this Article, member states have provide regulations that ensure that personal data is appropriately protected against loss, alteration, unauthorized disclosure or access, etc. It is, however, important to note that the appropriateness of such measures (and thus the necessity for implementing them) is always to be evaluated against the costs that would arise from their implementation and the data protection risks that arise from the processing etc. of personal data: "Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

This weighing between the risks for the data subject's rights to be infringed and the costs that would arise from the measures for protecting these rights from being infringed can only be made on a case-to-case basis, depending on factors like the concrete types of data that are to be collected, processed and used, the specific purposes behind this collection etc., the specific processes and system architectures being employed, etc. If, for instance, health data is to be collected, processed and used, this implies a different outcome of the appropriateness-weighing than it is the case for, for example, the customer data of an online shop, leading to even elaborate and costly security measures being deemed "appropriate" for the case of health data but not in the case of "simple" customer data. Depending on the type of the online shop, however, even such customer data may lead to a significant risk for the data subject's data protection rights. In certain cases, extensive security mechanisms may therefore be deemed appropriate (and thus compulsory) for customer data, too.

As already outlined above, this strongly speaks against the principle of data security being treated on the basis of generic certificates or privacy seals. Instead, the security mechanisms to be employed have to be

identified with specific regard to the respective case, thereby raising the problem of proving that certain measures have actually be taken and are in place for a specific, potentially risky collection, processing and use of personal data. A cloud user who has to prove this "being-in-place" of sophisticated but necessary security measures that go beyond the "base level" that is approved by generic certificates or privacy seals to, say, a data protection authority or the data subject, can currently hardly prove this on the basis of the information given to him from the cloud provider. Some of the technologies that are to be developed within the project SECCRIT, in turn, promise to fill this gap and to thereby make, on closer inspection, cloud computing a viable option for certain use cases in the first place.

3.3.10.2 European Legislation – General Data Protection Regulation

Art. 23 (1) indicates that the controller has to implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of the data protection regulation and ensure the protection of the data subject. As already discussed above, these can hardly be performed by the cloud user who is mostly considered as the controller. The option of introducing certificates and privacy seals (Art. 39) already discussed above, might provide some basic confidence of meeting at least fundamental security requirements but does not suffice especially in cases that require a thoughtful weighing between data protection risks and costs.

Regarding the problem that a cloud user can usually not exert any influence on the cloud providers actual practices (and thereby has only limited influence on the security measures being employed), the provision that the processor has to implement the technical and organizational measures together with the controller (Art. 30) at least go into the right direction. It remains to be seen how this obligation will influence actual practices as compared to the current state of the cloud provider determining all measures on his own and leaving the (potential) cloud user with a take-it-or-leave-it offer.

3.3.10.3 National Law – The German Example

Section 9 BDSG is referring to the adherence of the technical and organizational measures, imposing the controller the obligation for fulfilling this provision. The German national law basically matches the European directive discussed above without major specifics. The problem of weighing the case-specific risk and the costs arising from security measures therefore applies here, too, as well as all the above-mentioned implications from this do.

3.3.10.4 Data Security and Cloud Computing – Summary and Implications

In summary, cloud computing systems must be secured in order to prohibit an encroachment on the rights of the data subject. Therefore the controller has to ensure that appropriate technical and organizational measures have been taken for protecting personal data. As this task is thus to be done by the cloud user, this leads to significant problems. The cloud user cannot be in full control of the whole technological setting and he cannot be sure that specific security mechanisms are in place, configured properly and working correctly. In the lack of transparency this seems quite challenging for the cloud user to assure these measures to be taken. As certificates will never give this needed assurance, a suitable (technical) way will have to be found in order to simplify the possibility of guaranteeing the expected level of security.

3.3.11 User Rights / Supervision and Cloud Computing

Besides the provisions mentioned so far, the data subject also has a right for access to the data relating to him/her as well as a right for correction, deletion and blocking of his/her data. By these provisions, it shall be ensured that the data subject does not suffer detriments that result from inaccurate personal data

being used or from (albeit accurate) data being processed and used illegitimately. The mentioned user rights therefore provide instruments for interventions by means of which the data subject can – at least to a certain extent – ensure that the personal data related to him/her is treated in accordance with the provisions of data protection law. With regard to the specific givens of cloud computing, it is however yet unclear how these user rights are to be exerted in multi-personal-relationships involving at least the data subject, a cloud user and a cloud provider, where the cloud user is the only party known by the data subject while the cloud provider might in some cases be the more appropriate subject of interventions. It will have to be examined in more detail, under what conditions the cloud user as the only instance known to the data subject suffices as addressee of user-driven interventions and what technical mechanisms might be employed to strengthen the user's position in such settings.

Closely coupled with these user rights for inspection and intervention is the concept of (external) supervision, which refers to the existence of a dedicated party that is entitled to check whether the obligations of data protection laws are actually complied with. On the one hand, this supervision can be exerted internally within the organization that collects, processes and uses personal data (by a corporate data protection officer, for example), on the other hand, there always is an external party like a data protection authority which (also) is responsible for supervising the adherence of data protection laws. In particular, these parties shall ensure the compliance with regulation related to data protection by means of conducting periodical inspections, reviewing processes as well as technical and organizational means being employed during the collection, processing and use of personal data, and by providing a contact point for data subjects and other stakeholders to approach in case of wanting to lodge a complaint with regard to a certain party's practices of collecting, processing and using their personal data. The principle of having a dedicated party which is entitled to supervise the compliance with data protection laws, however, only makes sense if this party is also entitled to impose penalties in the case of noncompliance. In this regard, the different legal frameworks discussed below differ significantly.

Furthermore, the specific givens of cloud computing raise the problem of responsibility with regard to the exertion of external supervision. Given that the cloud provider and the cloud user reside in different countries, it has to be answered which data protection authority is responsible for exerting external supervision regarding a specific process of collecting, processing and using personal data.

3.3.11.1 European Legislation – Data Protection Directive

In the current data protection directive, the data subject's rights for access, rectification, erasure or blocking are codified in Art. 12. The existence of a dedicated party which is entitled to oversee the compliance with data protection laws is provided by art. 28, stating that "[e]ach Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States [...]", warranting this authority with complete independence, and providing them with powers for investigations, intervention and for carrying cases related to the assumed noncompliance with data protection laws to the courts. The supervisory authority is according to art. 28 always the one locally responsible at the place of the establishment of the controller.

3.3.11.2 European Legislation – General Data Protection Regulation

In the draft for a general data protection regulation, the data subject's rights are covered by chapter III. Besides the already mentioned rights for information and access, art. 16ff are focused on the rights for rectification and erasure. Further on the data subject has a right to object against the processing of personal data relating to him as long as there are no compulsory reasons for the processing (art. 19).

Art. 17 furthermore proclaims a right for the data subject to be forgotten and for the respective personal data to be erased. It seems, however, quite difficult for the data subject to actually assert this right in the cases when the data subject is not the cloud user but rather a client of the cloud user, especially when he – as it can usually be assumed – even doesn't know the cloud provider. If the concept of cloud computing is qualified as "acting on behalf of the controller" (see section 3.3.3 above), then the data subject's rights are to be entitled against the cloud user, who in turn has to be taken into account.[132] In the following, it is assumed that this way can actually be taken by the data subject because Art. 26 (2e) is obliging the processor to create together with the controller the necessary technical and organizational requirements for the fulfillment of the controller's obligation to respond to the requests for exercising the data subject's rights laid down in Chapter III, already mentioned above.

This would, however, cause follow-up problems as the cloud user is less informed about the internal functioning of processing than the processor and has no direct insight in what is actually happening to the data. Furthermore, the cloud user cannot give the guarantee that the data have, for example, been deleted and are not accessible to the cloud provider anymore. In this regard, art. 13 formulates an obligation for the initial controller to inform each recipient to whom the data have been disclosed about any rectification or erasure carried out in accordance with the art. 16 and 17. In the German law, however, it is generally accepted that "acting as a processor" is not counting as "acting as a recipient".[133] It has to be determined whether this will also be the case on the European level once the general data protection regulation becomes effective. If so, this would imply that the processor needs a separate legitimation, that he has to inform the data subject about the specifics of the processing, etc. (see section 3.3.3 and 3.3.9)

In addition to these user rights, art. 18 formulates a novel right to data portability, which means that the data subject has a right to receive a copy of his data. This data portability basically emanates from the observation that especially users of social networks (as indicated in the recital 55) or employees have a vital interest in the preservation and reuse of their data even in the case of not being connected to the respective holder of the data anymore. With regard to cloud computing, this regulatory concept of art. 18 could become highly relevant in the case of the cloud provider being changed. In multi-personal relationships, however, we can again expect the same type of problems as above because of the ultimate holder of the data usually not being known by the data subject. Nonetheless a respective contractual basement could be a possible option here.[134] The cloud user, in turn, cannot profit from this regulation in matters of easing the change of a cloud provider, because he is no natural person and thus the regulations do not provide him with a comparable right for portability.

Regarding the role of supervision being exerted, the draft for a general data protection regulation indicates that the supervisory authority can exercise the powers conferred on it on the territory of its own member state in accordance to art. 53. When the controller has multiple establishments in different member states, the supervisory authority of the main establishment comes into force for all the other member states, art. 51 (2). If there is no main establishment within the EU, a supervisory authority has to be named. According to art. 4 no. 13 p. 1, this is the one responsible for the place where the processing takes place.

3.3.11.3 National Law – The German Example

As the German BDSG covers not only commercial companies but also public and private bodies, there are multiple regulations dedicated to the user rights. There is in particular a general provision in Section 6

[132] S. Gola/Schomerus, section 11, recital 4.
[133] Erbs/Kohlhaas-Ambs, Strafrechtliche Nebengesetzte, 192. edition 2012, D.7.25.
[134] Hornung/Sädtler, Europas Wolken, CR 10/2012, 638, 641.

while from Section 19 to 21 there is one for the processing by public bodies and in Section 33 to 35 for private bodies and commercial enterprises. Supervision of compliance with data protection laws is regulated in section 38 (6), providing that the land governments or the bodies authorized designate the supervisory authorities. For the Land Baden-Württemberg this is, for example, coordinated by the "Landesdatenschutzbeauftragter" within the regulations in section 26ff LDSG.

3.3.11.4 User Rights/Supervision and Cloud Computing – Summary and Implications

The user rights of the data subject have to be safeguarded by the cloud user. The enforcement of these rights however requires a certain contribution of the cloud provider as he possesses the personal data. It seems, however, quite difficult for the data subject to actually assert these rights when the data are in the sphere of the cloud provider. If, for example, a cloud user's client wants his personal data to be erased by the cloud user, this raises substantial problems for the cloud user as he cannot be sure what the cloud provider actually did and does with the respective data – it could, for example, have been backed up automatically several times before or the cloud provider could even not actually delete this data but only mask them out of the cloud user's database view. In any case, it would seem more appropriate to make the cloud provider (also) the subject of interventions. This will however have to be examined in more detail throughout the SECCRIT project time. Furthermore the data subject has the possibility to approach the supervisory authority whenever his rights seem to be infracted.

3.4 Data Protection Law and Cloud Computing – Conclusion

Altogether, it can be stated that a number of significant problems can be revealed when the concept of cloud computing is critically and thoroughly assessed against the givens of data protection law, vividly illustrating that the law has (again) still not caught up with technical innovation. While the existing provisions are not functioning as originally intended with regard to cloud computing, there is a real and significant lack of protection for the data subject which can lead to a factual encroachment of fundamental rights like the right to informational self-determination.

In particular in multi-personal relationships – which are omnipresent in the field of cloud computing – the absence of transparency and the fact that access rights have to be realized by the controller are still the main barrier. If the cloud provider is legally understood as acting on behalf of the cloud user as a processor, then the cloud user remains the responsible party for the adherence of data protection rules, even though he does not know what is actually happening with the data and even if these data are completely in the sphere of the cloud provider without the cloud user being able to actually influence the concrete conditions of the collection, processing and use of that data. Admittedly, the concept of "processing on behalf of the controller" concedes the controller the right of instructing the processor and also, in order to accomplish his duty of maintaining "appropriate" technical and organizational measures for the protecting, a right for inspection, but both are associated with constitutive difficulties in practice, of which only be the latter one could be softened assured by means of certificates or seals being issued by third parties.

Given these and further deficiencies outlined above, it becomes highly questionable whether the concept of "processing on behalf of the controller" actually is a suitable option for the legal characterization of cloud computing. A comparable issue arises with regard to the legitimation, which is always a necessary precondition for any collection, processing or use of personal data. Here, the individual consent as well as the balance of rights and interests (which will always have to be weighed against each other on a case-by-case basis) both prove rather unsuited when they should be applied to cloud computing, again revealing significant gaps in the current regulatory framework.

Alongside, the Cloud Provider has to ensure an adequate level of data protection and it has to be warranted, probably by means of contracts, that the provider only processes the data for the purpose they have been collected for. In addition, there is a real disequilibrium between a small or medium-sized company and a well-known cloud provider, so the influence of the cloud user on the cloud provider will only be regulated on a contractual basis. This is certainly not conformant to the grit imagined by the legislator. It has to be assured that the cloud provider really ensures the existence of technical and organizational security measures and that the data subjects do not have to fear an encroachment of their rights. For now this can only be done by means of standard contracts. The actual compliance with such regulations, in turn, can neither be examined by the cloud user nor proven by the cloud provider today. Some of the technologies that are to be developed during the project SECCRIT might prove highly valuable in this regard.

The data protection regulation draft currently discussed on the European level also offers no viable solutions for these (and other) cloud-specific challenges with regard to data protection. Especially concerning the multi-personal relationships many of the existing as well as of the currently discussed rules are not suitable. In the end, many of the current regulations are actually not suitable for being applied to cloud computing as it is understood from the technological perspective. It will have to be determined throughout the SECCRIT project, how the existing regulations can be brought into accordance with the technical concepts driving the omnipresent – and in many regards desirable – trend towards cloud computing.

3.5 Documentation of Exchange with Data Protection Authorities etc.

The continuous involvement of relevant regulatory bodies is integral for the success of the overall project and, in particular, for ensuring the practical applicability of developed technical solutions. In this regard the following activities have already been initiated:

- The German Federal Data Protection Officer was contacted and invited to join the User and Advisory Board. After some promising exchange in March and April 2013, the Data Protection Office had to refuse the invitation because of “scarce resources and at the same time increasing duties” on April 11, 2013. The responsible assistant did, however, ask to be kept up to date and will be done so.

- The German Physikalisch-Technische Bundesanstalt (PTB), which is responsible for providing technical specifications on the collection and processing of any kind of measurement data was invited to the User and Advisory Board and happily joined it. As the PTB is, in particular, responsible for regulations on the processing of energy data, this provides promising opportunities for upcoming challenges in the field of data-protection-friendly collection and processing of smart meter data in the cloud to be considered from an early stage of project SECCRIT.

- The Austrian data protection activist group “quintessenz.at”, which also organizes the Austrian “Big Brother Award” was also invited to the User and Advisory Board and joined it in June 2013. The establishment of close exchange is currently gaining momentum.

- With the local data protection authorities of Finland and Spain, where the project’s demonstrators are to be located, no close exchange has been established yet. The reason lies in the fact that these data protection authorities should assess the aspired project scenarios. This is, however, only possible with sufficiently detailed descriptions of the scenarios to be assessed which, different from the original project plan, were only finalized during June 2013 (M6). The

exchange over the now available concrete scenarios will, however, be initiated immediately after the M6 deadline by the local project partners in Finland and Spain. A report on this exchange will be included in D2.4 “National data Protection Consultation Results”.

Furthermore, the project members will use any additional chance for establishing a more intense contact with other regulatory bodies from the relevant fields whenever such opportunities arise during daily course, events etc.

4 Summary

Altogether the main legal fundamentals concerning evidence and data protection law gained in this deliverable are the following:

Evidence Law:

- The cloud computing contract seems to be a lease contract.
- The cloud provider will possibly be responsible for hacker attacks and overloading.
- The cloud provider could possibly be someone who has been used by the cloud user in order to perform the owed obligations of that one.
- A credible technical evidence should be taken into account as the already existing (modalities of) evidence do not seem to properly work because of the lack of transparency.
- SLAs seem quite appropriate; for the cloud user it would be important to clarify the liability issues and the possible breach of duties. On the other hand too detailed clauses, which cannot be easily attained, can have their opposite effect.

Data Protection Law:

- The existing provisions are not functioning with cloud computing; there is a real lack of protection possibilities for the data subject.
- In multi-person-relationships the absence of transparency and the fact that the access rights have to be realized by the controller seems to lead to different problems.
- The cloud provider is usually assumed to “act on behalf of the controller“, the cloud user. That leads to the fact, that the cloud user is the only party responsible for the compliance with data protection rules, even though he does not know where the data and the processes are exactly outsourced to, as these are in the sphere of the cloud provider. Problematical seems also the fact that the cloud user has to instruct the cloud provider and check that he fulfills the duty of maintaining technical and organizational measures of data protection. For the latter one, expertises from independent third parties are usually assumed to be appropriate but are revealing problems regarding the need for case-to-case-weightings of appropriateness, for example. It will therefore have to be evaluated whether the “processing on behalf of the controller” is actually a suitable option for cloud computing.
- The individually given consent is not a practicable mode for providing legitimation, as the cloud provider would have to get this consent from every single data subject.
- The balance of rights is a case-by-case decision which possibly prevents the cloud user from relocating his data when the encroachment of fundamental rights like the right to informational self-determination could be offended.

The forthcoming legal deliverable will have to pick up those raised questions.

5 References

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

Bizer, Johann: Sieben goldene Regeln des Datenschutzes. In: DuD 2007, 350, 356.

Blaha, Ralf-Roland Marko-Andreas Zellhofer/Helmut Liebel: Rechtsfragen des Cloud Computing, Wien 2011.

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

Bräutigam, Peter: SLA: In der Praxis alles klar? In: CR 2004, 248-254.

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

Eckhardt, Jens: Rechtliche Grundlagen der IT-Sicherheit. In: DuD 2008, 330-336.

Eckhardt, Jens; Kramer, Rudi: EU-DSGVO- Diskussionspunkte aus der Praxis. In: DuD 2013, 287-294.

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

Erbs, Georg/Kohlhaas, Max: Strafrechtliche Nebengesetzte, 192. edition, München 2012.

Fritzemeyer, *Wolfgang*: Die rechtliche Einordnung von IT-Verträgen und deren Folgen. In: NJW 2011, 2918- 2922.

Gentry, Craig: Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st annual ACM symposium on Theory of computing, 2009, 169–178.

Giebichenstein, Rüdiger; Weiss, Andreas: Zertifizierte Cloud durch das EuroCloud Star Euro Audit SaaS Ein Best-Practice Ansatz zur Auswahl eines vertrauenswürdigen Cloud-Anbieters. In: DuD 2011, 338-342.

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

Grützner, Thomas; Jakob, Andreas: Compliance von A-Z, 1.edition, München 2010.

Hartung, Jürgen; Stiemerling, Oliver: Effektive Service-Level-Kriterien. In: CR 2011, 617-624.

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

Hennrich, Thorsten: Compliance in Clouds. In: CR 2011, 546-552.

Hoeren, Thomas; Sieber, Ulrich: Multimedia-Recht, 32. Edition, München 2012.

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

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

International Telecommunivation Union – Telecommunications Standardization Sector (ITU-T): Privacy in Cloud Computing- ITU-T Technology Watch Report, March 2012. Geneva, Switzerland: ITU.

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

Jessen, Tanja: Vertragsgestaltung und –praxis der Online Dienste. In: ZUM 1998, 282-292.

Jotzo, Florian: Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr? In: MMR 2009, 232-237.

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.

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

Kinne, Harald; Schach, Klaus; Bieber, Hans-Jürgen: Miet- und Mietprozessrecht, 6. edition Freiburg, Berlin, München 2011.

Koch, Frank: Application Service Providing als neue IT-Leistung. In: ITRB 2001 39-42.

Koch, Frank: Updating von Sicherheitssoftware – Haftung und Beweislast. In: CR 2009, 485-491.

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

Libertus, Michael: Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren. In: MMR 2005, 507-512.

Nägele, Thomas; Jacobs, Sven: Rechtsfragen des Cloud Computing. In: ZUM 2010, 281-292.

Niemann, Fabian; Paul, Jörg-Alexander: Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computings. In: K&R 2009, 444-452.

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

Palandt, Otto: Bürgerliches Gesetzbuch, 70. Edition, München 2010.

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

Schoolmann, Jürgen/Rieger, Holger: Praxishandbuch IT-Sicherheit, Risiken, Prozesse, Standards, 2005.

Schröder, Christian; Haag, Nils Christian: Stellungnahme der Art. 29-Datenschutzgruppe zum Cloud Computing. In: ZD 11/2012, 495-501.

Schulz, Carsten: Rechtliche Aspekte des Cloud Computing im Überblick, Inside the Cloud – Neue Herausforderungen für das Informationsrecht. Tagungsband zur DSRI Herbstakademie 2009, S. 403-418.

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.

Sieber, Ulrich: Haftung für Online-Datenbanken. In: CR 1992, 518-526.

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

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

Spies, Axel: EU/USA: Aktualisierte Standradvertragsklauseln für den internationalen Datentransfer. In: MMR-Aktuell 2010, 298882.

Splittgerber, Andreas; Rockstroh, Sebastian: Sicher durch die Cloud navigieren – Vertragsgestaltung beim Cloud Computing. In: BB 2011, 2179-2185.

Sripanidkulchai, Kunwadee; Sahu, Sambit; Ruan, Yaoping; Shaikh, Anes; Dorai, Chitra: Are Clouds Ready for Large Distributed Applications? LADIS 2009, also appeared at ACM SIGOPS Operating Systems Review, Volume 44, Issue 2, April 2010.

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.

Wybitul, Tim; Rauer, Nils: EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz. In: ZD 2012, 160, 164.

Zöller, Richard: Zivilprozessordnung, 28. Auflage, Köln 2009.