EU Expert Group on Cloud Computing Contracts

Questions for the Discussion on Subcontracting

Current practices and risks

1. Do cloud providers subcontract to one subcontractor or rather to a whole chain of subcontractors? How is currently the risk/liability shared among subcontractors within a chain? Do main providers/subcontractors use back-to-back contracts (i.e. do providers pass on the whole liability to a subcontractor) or retain some part? Do cloud providers know their subcontractors from the outset or rather subcontract their services only once needed?

2. Do cloud providers differentiate between subcontractors which are acting as processors of personal data and subcontractors which do not process personal data? Does such a distinction make sense from the provider’s perspective and/or from a user’s perspective?

3. What are the most important risks that consumers and small firms faced when the CSP uses subcontractors and sub-sub-contractor for performing the contracts? How can SMEs offering cloud services mitigate these risks?

Information about sub-contractors

4. Is information about sub-contractors important for cloud users? If so, why? If so, how much and what kind of information about sub-contractors (e.g. identity of all subcontractors, description of the scope of services subject to subcontracting, location of the subcontractor, conditions and terms of the subcontracts etc.) may cloud users expect from the CSP? Would these expectations differ if the user is an SME or a consumer? Would it be problematic for the CSP to provide to the cloud user such information?

5. Shall the end user agree to all sub-contractors? If so, why? Due to the large number of subcontractors normally involved for supply of cloud computing service, how could such authorisation be given?

6. Should an end user be informed of a new or a change of sub-contractor? If so, why? Always or only in specific circumstances (e.g. when a change of contractor impact the level of service provided to the end user; change of localisation of the sub-contractor)? If so, how should the end-user be informed? Should the end user be able to refuse such change? If so, why?

7. Does the situation differ for subcontracting involving processing of personal data? If so, how?

Liability

8. How do your existing national laws regulate liability of subcontractors of cloud contracts? Would the internal distribution of risk/liability between provider and subcontractors have an influence on the liability of the provider towards the user and corresponding user’s rights?
# Cloud Computing Contracts – Discussion Paper on Subcontracting

Draft – March 25, 2014

Authors: Isabell Conrad, Maria-Urania Dovas, Federica Poggioli, Robert Selk, Susann Wolfgram

## Table of Contents:

A. Overview, Summary, Conclusions and Recommendations ................................................................. 3

I. Introduction ........................................................................................................................................ 3

II. “Internal” and “External” Subprocessors ............................................................................................. 3

III. Applicability of Binding Corporate Rules for Processors to external Sub-processors ....................... 4

IV. Commercial Aspects of Customer Data ............................................................................................... 4

V. Risks of Subprocessing and contractual Solutions ............................................................................. 4

VI. Technical and Organizational Measures .......................................................................................... 4

VII. Technical Recommendations ........................................................................................................... 4

VIII. EU Model Clauses for Subcontracting .......................................................................................... 5

IX. Certification as a Solution .................................................................................................................. 5

X. Aspects of Equipment and Product Safety and comparable Solutions for Subcontracting in Cloud Computing ................................................................. 5

B. Business Models ................................................................................................................................... 7

I. Combination of the Cloud Service Types (SaaS, IaaS, PaaS etc.) by Subcontracting and CSP Chains ........ 7

II. Types of Third Party CSP: Freelancer, Third Party / OS Software Provider, Consortium Partner, Distribution Partner, Maintenance Provider ........................................................................................................ 7

III. General Contractorship versus Multilateral Contracts and Bilateral Contracts with Clusters of Providers ........................................................................................................................................ 7

IV. Types of Subcontracting Clauses: General Permission versus Consent/Permission in Individual Cases versus No Contractual Regulation ........................................................................................................... 8

V. Differences between SaaS, IaaS, PaaS? ............................................................................................... 9

VI. Differences between B2C and B2B? ...................................................................................................... 9

C. Subcontracting – Risks and Benefits .................................................................................................. 9

I. Risks ...................................................................................................................................................... 9

II. Benefits ............................................................................................................................................... 11

D. Critical Links between End Customer Contract and Subcontractor Contract ........................................... 12

I. Consistency of Contractual Provisions ................................................................................................. 12

II. Description/Specification of Service ................................................................................................... 12

III. Service Levels/Time Zone Differences .............................................................................................. 12

IV. Cooperation Duties/Active Involvement of the Customer .................................................................. 13

V. Change Management/Change Request/ Data Protection Instructions of the Controller ................. 13

VI. Subcontracting and IP ......................................................................................................................... 13

VII. Warranty and Liability ...................................................................................................................... 13

VIII. Subcontracting and Antitrust Law (internal/external Subprocessors) .............................................. 13

IX. Termination of the contract ................................................................................................................ 13

E. Requirements from a Data Protection Law Perspective ........................................................................ 14

I. Statutory Regulation ............................................................................................................................. 14

II. Interplay of Data Protection Law and Contract Law ......................................................................... 16

F. Specific Issues for Persons Subject to Professional Secrecy (e.g. Attorney Client Privilege) ................ 17

I. Overview .............................................................................................................................................. 17

II. Use of Cloud Services by Lawyers ................................................................................................... 17

Annex 1 .................................................................................................................................................... 18

Annex 2 .................................................................................................................................................... 20

Detailed further Questions ........................................................................................................................ 27
A. Overview, Summary, Conclusions and Recommendations

I. Introduction

Cloud Computing for Consumers and Small & Medium Enterprises (SME) has become unthinkable without subcontracting. Subcontracting comes in various shapes and constellations. Either a company is in need for a short-term extension of its storage capacities or it is systematically outsourcing parts of its own services to subcontractors mainly for economical / business reasons. In some business models several Cloud Service Providers (CSPs) form a consortium where services are allocated to different companies and the possibilities do not end here. More than any other IT service, Cloud Computing for Consumers / SME has a very strong cross-border character (follow-the-sun), especially where subcontractors are involved and data may be shared across different regions in different (or unknown) data centres. Furthermore, the perception of a permanent service availability (24x7) or other high service level commitments may make a global provision of Cloud Services (for technical support, maintenance, storage) unavoidable. As the CSP is likely not to be able to tailor the delivery of Services just to one customer (except for private cloud solutions – which in general do not apply for Consumer/SME), it is an inherent pre-condition for CSPs to run their business and engage subcontractors as they see fit under certain conditions.

From a customer perspective, subcontracting in general bears two types of Cloud related risks that they must consider:
- data related risks and
- performance related risks (which often but not necessarily are closely entwined with data related risks).

Consequently, subcontracting in Cloud Computing raises major issues under EU and Member State law in particular regarding contract law and regulatory law with regard to data (such as data protection – in general and branch specific like health care -, aspects of professional secrecy, business & trade secrets, tax and accounting requirements, etc.). Other legal issues of subcontracting result from copyright law or export control regulations (e.g., where data is encrypted to minimize data protection issues as encryption technology is not per se admissible in all countries).

Subcontracting is interwoven with other topics which have been subject of previous meeting of the EU Expert Group on Cloud Computing Contracts such as
- data location, data access and data security or
- modifications of the contracts (e.g. due to fluctuation subcontracts).

This Discussion Paper focuses on legal issues of subcontracting which are not subject of other Discussion Papers.

II. Distinction between regulatory requirements for data processing and other risks

From a regulation point of view, a clear distinction is necessary regarding subcontracting, as to whether or not it involves processing of or access to customer data protected under data protection law (Sub-processing) or other data specific law such as professional secrecy. Many concerns of consumers/SME only apply in the area of Sub-processing, professional secrecy, business & trade secrets, tax requirements and similar issues. In general, it is not of interest or concern to the consumer / SME to know which subcontractors (e.g. hardware vendors, software providers, telecommunication providers etc.) the CSP utilizes as long as it provides the consumer/SME with the agreed and adequate availability / performance and security. Performance and security related risks can be reduced by internationally accepted IT standards and certifications and clear responsibility and liability in the contract (see below V. et seq.).

In contrast, according to European and national law Cloud related risks of the end customer resulting from data related regulatory acts (such as Controllership of personal data or professional secrecy) cannot be shifted to the CSP by contractual clauses (responsibility, warranty / Service Level Agreements, liability) or minimized by proof of standards and certifications by the CSP. This is the greatest impediment for Cloud Computing in the EU. Therefore, this Discussion Paper has a strong focus on data protection (Subprocessing) and professional secrecy (in case of small law firm or small doctor's practices etc.) as examples for data related restrictions applicable for Cloud Services.

III. “Internal” and “External” Subprocessors

Only the largest CSPs can – theoretically – afford to provide those Cloud Services without using (external) subcontractors. In general, even big multinational providers include at least affiliates (other members of their corporate group) in their Cloud Services (internal subcontractors). In particular, from a data protection and professional secrecy perspective, Cloud Computing could be promoted in the EU if the EU Commission (e.g. in the Draft of the General Data Protection Regulation) developed a (new) privilege for Controllers (and
Processors) so that Processors may subcontract affiliates or certified external Subs, Subsubs and Sub-subsubs, which guarantee a level of technical and organizational measures comparable with and as adequate as the Processor’s level. Under the present national data protection law and according to the drafts of the General Data Protection Regulation (EU Commission and LIBE), chains of Subprocessors are hardly solvable as the Controller must retain full Controllership (e.g. conduct audits even at locations of foreign Subsubs – which can be done only theoretically). Therefore, it is interesting to evaluate if CSP’s affiliates and external Subprocessors with adequate data protection and security standards in place should be treated differently than any other third party Subprocessors. Bilateral contracts between the CSP and each affiliate are challenging to administer – even with Binding Corporate Rules for Processors (a new model developed by the Art. 29 Working Party, which is effective since 2013).

IV. Applicability of Binding Corporate Rules for Processors to external Sub-subprocessors

An alternative would be applying Binding Corporate Rules, which are currently only applicable within a group of companies, to data transfer to the cloud, including non-EU subcontractors. The obstacle in this solution is the fact that the binding nature of such BCR for the participating Cloud Service providers must be ensured. This is not yet the case.

Furthermore, although Binding Corporate Rules for Processors are a helpful tool to consider in connection with Cloud Computing, the question remains whether or not this instrument is applicable for chains of Subprocessors. Working Paper 195 of the Article 29 Working Party expressly distinguishes between “internal” Subprocessors, i.e. Subprocessors that are part of a corporate group on the one hand “external” Subprocessors on the other, i.e. entities outside a corporate group. However, it remains unclear whether an external Sub-subprocessor should be included by the definition of an external Subprocessor as well, thus benefiting from Binding Corporate Rules for Processors.

V. Risks of Subprocessing and contractual Solutions

Certain contractual restrictions can serve to address the main concerns of consumers/SME, such as:

- Same legal responsibility for acts and omissions of the subcontractor/Subprocessor;
- Pass on contractual obligations to subcontractor/Subprocessor, as relevant but not less restrictive

Additional obligations for Subprocessors:

- Transparent selection, on-going training and monitoring process by CSP vis-à-vis Subprocessor;
- Disclosure of names and roles of Subprocessors (at least annually / upon request of the consumer/SME);
- Process to change (remove/add) suitable Subprocessors, e.g.:
  - Email notice by CSP and description of change;
  - Change accepted if Consumer/SME does not object within a reasonable time-period (e.g. 30 days). In case of objection, either party should be granted an optional termination of the Cloud Agreement if CSP is unable to administer or offer exceptional treatment for the objecting consumer/SME. Should such termination right be limited to defined reasons, e.g. if the new Subprocessor is based outside the EEA (even if the Subprocessor contractually or by law provides for an adequate level of data protection)?
  - Consumer/SME to rely on audits / certifications of Subprocessor by CSP and authorize the CSP as the data processor to fulfil the control requirements of an SME as the data controller vis-à-vis any Subprocessor.

VI. Technical and Organizational Measures

Another solution could be a similar approach as the one followed by the German legislator in creating a catalogue for data processing, where data processors were required to list their technical and organizational measures, so the data controller could verify them. In practice, however, a large number of service providers are unable to fulfill the requirements of German law and to describe their own measures. There is no (written) security concept, which a data controller could adequately check and many data processing agreements lack of specific security measures, although many DPAs have published model data processing agreements with concrete examples.

VII. Technical Recommendations

Technical recommendations can be another way of dealing with Cloud Computing and offering equal chances to providers throughout the EU. It must be kept in mind, though, that smaller companies can only provide their services by subcontracting non-EU Cloud Service providers, with a significant fluctuation. This poses difficulties in enforcing and checking norms and standards. In this respect, this problem is comparable to data
export to the USA and Safe Harbor certification, where EU DPAs do not consider it sufficient that certified US companies are included in a Safe Harbor list available online. Nevertheless, especially regarding the protection of personal data and confidential business data of the customer it is important to develop norms and standards, etc. i.e. data which have been transferred to the cloud can be (verifiably) erased.

VIII. EU Model Clauses for Subcontracting

On a contract law level a model comparable to the EU Model /or policies / standards to be incorporated into the Cloud Service agreement for various cloud constellations, as applicable and suitable, seems recommendable which can be used on a voluntary basis. Especially for tackling the problem of subcontractors in non-EU countries, the creation of EU Model Clauses especially for cloud computing should be considered. These could be constructed along the lines of the controller-to-processor Clauses from 2010, but should especially take into account that possibly fluctuating subcontractors in non-EU countries and possibly larger supply chains are or can be commissioned. In view of this fact, the cloud model clauses should also regulate for cases of subcontracting with non-EU countries, whether the model agreement should be executed between the data exporter and its direct contractual partner, i.e. the CSP or between the data exporter and the subcontractor. This solution reaches its limits in cloud computing, though, where neither customers nor subcontractors have much interest in concluding dozens of agreements, where they will need to react to any minor changes on the subcontractor’s side. There is, further to this, need for legislative activity, as these contracts would require execution in written form, which is not practicable especially for public cloud solutions, where commissioning, change and termination is usually effected with electronic means.

IX. Certification as a Solution

Considering Cloud Computing and Big Data it is one of the most important tasks of modern data protection law to create international incentives for the development of new data protection friendly techniques and to request action not only from data processors but from IT manufacturers as well. Standardized provisions and (technical) norms or recommendations for Cloud Computing are thus a step into the right direction as they provide for legal certainty. The European Commission should observe and include international certifications in these considerations, since there is already much experience in companies and in practice. These considerations could include recognized certifications such as ISO 27000 and 27001 or SSAE16, which could be turned into a part of the “EU Cloud Certification”.

X. Aspects of Equipment and Product Safety and comparable Solutions for Subcontracting in Cloud Computing

Under European data protection law, the Data Controller cannot rid himself of the responsibility for controllership of the data under any circumstances. Compared to other contractual situations, where the end customer finds himself at the very end of a supply chain he can neither oversee nor influence, this is rather unsatisfactory. This Discussion paper comes to the conclusion that is also a great obstacle to subcontracting in Cloud Computing. In order to tackle this situation, it might be helpful to implement aspects of equipment and product safety law into the requirements for Cloud Computing subcontracting and into data protection law in general. Of course, Cloud Computing rarely leads to health risks for the end customer. However, the Consumer’s and SME’s incapability to control their data processed in the Cloud is in some aspects comparable to equipment and product safety situations. It might be acceptable for the Cloud Service Providers (also SMEs) to accept these standards if they are discharged of individual requests by each consumer/customer and can rather generally “certify” their solution as such. The consequences could be

- less responsibility for the customer / Controller;
- more obligations for the “product manufacturer” (CSP);
- (yearly) certification obligations, proofs of a valid certification and traceability in the supply chain (in lieu of individual audit rights of consumers (not data subjects that are granted constitutional rights) or potentially even authorities);
- recourse rights for the members of the supply chain if a customer asserts claims against the CSP;
- as a benefit for the CSPs they should be relatively free to subcontract to such certified Subs and Sub-sub’s and the Controller should have no obligations to audit/ inspect the supply chain.

There are comparable legislative solutions in place for other areas of business, e.g. machinery. Directive 2006/42/EC on machinery states in recital 19:

"In view of the nature of the risks involved in the use of machinery covered by this Directive, procedures for assessing conformity to the essential health and safety requirements should be established. These procedures should be devised in the light of the extent of the danger inherent in such machinery. Consequently, each category of machinery should have its appropriate procedure in conformity with Council Decision 93/465/EEC of 22 July 1993 concerning the modules for the various phases of the conformity
assessment procedures and the rules for the affixing and use of the CE conformity marking, which are intended to be used in the technical harmonisation directives (2), taking account of the nature of the verification required for such machinery.”

These principles could be adapted to Cloud Computing and the risks involved in subcontracting. The Directive continues in recitals 22 and 23:

“(22) In order to ensure the same quality for the CE marking and the manufacturer’s mark, it is important that they be affixed according to the same techniques. In order to avoid confusion between any CE markings which might appear on certain components and the CE marking corresponding to the machinery, it is important that the latter marking be affixed alongside the name of the person who has taken responsibility for it, namely the manufacturer or his authorised representative.

(23) The manufacturer or his authorised representative should also ensure that a risk assessment is carried out for the machinery which he wishes to place on the market. For this purpose, he should determine which are the essential health and safety requirements applicable to his machinery and in respect of which he must take measures.”

As the situation is today, the data protection authorities in the Member States have neither the capacities to conduct such certifications nor are they free of conflict of interests. In order to achieve a certain level of security and to distribute responsibilities and liabilities evenly within the supply chain, a self-certification system comparable to that for machinery could be introduced according to the guidelines set out above. This concept is not new to data protection, but its field of application could be considerably extended.

Taking no action at all and waiting for the General Data Protection Regulation to come into force is not an option. Although the intention of this Regulation is to provide for full harmonization within the EU and it will thus simplify the provision of Cloud Services within the EU, it is not unlikely that it will lead to an increasing discrepancy between EU data protection law and data protection law in “uncertain third countries”. 
B. Business Models

I. Combination of the Cloud Service Types (SaaS, IaaS, PaaS etc.) by Subcontracting and CSP Chains

II. Types of Third Party CSP: Freelancer, Third Party / OS Software Provider, Consortium Partner, Distribution Partner, Maintenance Provider

1. A difference between the contractual (civil law) side on the one hand and a technical approach (privacy by design) one the other hand seems to be useful:

a. Regarding the contractual /civil law side, making differences for the different types of subcontractors is increasing the complexity of standard contractual clauses. The customers usually do not make any difference regarding the type of subcontractors; for them only their contractual partner should be liable and responsible for all data processing, irrespective of what kind of sub-contract is in place with a subcontractor. In other words, if a customer is not fine with involving a subcontractor, there is a high chance it will reject the involvement of any type of subcontractor.

b. From a data security point of view there could be an important difference: The smaller and the more “personal” (freelancer, small companies run by one owner) a subcontractor is, the more the contracting parties must control this subcontractor, particularly the CSP as the direct contracting party of the subcontractor.

c. Furthermore, the more services outsourced to a subcontractor are processing (personal or sensitive) data stored in the cloud, the stricter the technical and organizational measures have to be.

d. Subcontractors involved in the distribution of the services only, not in the processing of any kind of data as part of the cloud computing, could be handled in a more relaxed way: Neither have they access to the data nor do they influence the processing of the data and services; they “just” sell the services, provided by third parties. They should thus not be considered as subcontractors, they are part of the sales organisation of the CSP, similar to a broker or agent.

2. Suggestion: Obligation of the CSP to develop a matrix and fill in the different kinds of subcontractors, their roles and locations, depending on risk class/impact chances (risk-based approach).

III. General Contractorship versus Multilateral Contracts and Bilateral Contracts with Clusters of Providers

All of these approaches have different advantages and disadvantages depending on the point of view:

1. The customers of CSP are usually interested in having general contractorship contracts in place to shift the task as well as the risk of coordinating the different subcontractors to the CSP. In many cases, only the CSP is able to do so and it is in its interest as well.
2. Multilateral cloud contracts would have – if any – a very small applicable field of business. Besides, it would not be a subcontracting situation any more if there were direct contracts among all stakeholders involved.

3. Having a situation with multi party agreements in such a way that each party has more than one contracting partner will lead to a very complex legal situation and liability situation. The aim of drafting simple standard contractual clauses will be hard to achieve. On the other hand, a mutually applicable “framework” or “standard” (e.g. issued by the European Commission similar to the bilateral EU Model Clauses) that the parties agree to adhere to may accomplish simplicity in the contractual set up (a simple reference in the Cloud service agreement that incorporates these terms would be sufficient). At the same time, it may secure the direct relationship between the contracting parties and guarantee a transparent, consistent level of contractual and data security.

4. Even a cluster of providers needs to be based on a legal construction and therefore one entity acting for the whole cluster:
   a. Working with a power of attorney (one CSP of the cluster is acting on behalf of each of the other members) will lead to many single contracts with many, usually unknown contracting partners.
   b. Considering the cluster as one (legal) entity will not work because a legal construction has to be found which cannot be done by standard contractual clauses between the customer and the CSP (and will have a lot of further impact, for example by tax laws)

IV. Types of Subcontracting Clauses: General Permission versus Consent/Permission in Individual Cases versus No Contractual Regulation

1. As further illustrated in the example subprocessing/subcontracting provisions attached in Annex 1, such clauses can vary by provider but typically address (a subset of) the following:
   a. Assumption of legal responsibility for subprocessor/subcontractor
   b. Potential restrictions/requirements to engage subprocessors/subcontractors versus free assignment/engagement of such third parties: consent, notice or mere information of then-current subprocessors/subcontractors used upon request
   c. Potential restrictions to engage in multi-tiered subprocessing, i.e. restriction to further subcontract by (authorized/approved/appointed) subprocessors
   d. Contractual obligations of a similar protection in (written) subprocessing agreements
   e. Remedies/exit rights by either/both parties in case of changes or breach of contractual obligations by a subprocessor
   f. Third party beneficiary clauses or other means to ensure cooperation/information (e.g. in case of security breaches) and legal enforcement of data protection obligations against subprocessors/subcontractors

2. Seeing only the civil law side, the solution of “no contractual regulations” could be a simple choice. As long as the CSP is liable in the relationship to the customer, there will be no disadvantage for the customer from that point of view.

3. However, most probably personal data will be part of a Cloud Service, either because the data stored in the cloud consists of personal data or because personal data regarding the people working in the cloud software will be logged and stored. Because of the data protection requirements, this option will not be a solution. As long as the customer is the data owner and the controller (and the CSP is only the processor), there is a strong interest for the customer to know any subcontractors, as well as the chance of not only knowing the subcontractors but to have the possibility to give (or to deny) a consent.

4. For reasons of clarity, a general permission is better than “no regulations”. By giving general permission, the customer is at least aware of the subcontracting situation. Because the data involved is customer’s data, there is a need for that.

5. A compromise is to include a general permission in the contract and to have a list of the subcontractors that will be or could be involved. The question is, however, how to change this list if subcontractors change: By informing each contracting partner individually? By publishing the changes on a website?
V. **Differences between SaaS, IaaS, PaaS?**

1. This distinction provides no advantages: Either a customer agrees with the involvement of subcontractors or it disagrees. Customers usually do not differentiate between the service itself (Saas) and/or the infrastructure the service is running on.

2. A possible differentiator could be the question whether there is a possibility for the subcontractor to access any data stored in the cloud or not.

VI. **Differences between B2C and B2B?**

1. From a legal point of view, there is no difference: Either a cloud provider is providing all offered services on its own or he needs or wants to involve Subprocessors because it lacks the required resources, expertise or cost efficiencies. Thus, from a legal point of view there is no difference between the two types of customers. All the more as every Cloud Service Provider will want to use third party Subprocessors in one way or the other at some point in time and hence it is doubtful that there is a real market offer of Cloud Services without subcontractors/subprocessors.

2. From a business point of view, B2C-customers usually have less interest in knowing the involved Subprocessors than B2B-customers: The B2B-customers may have to meet internal policies or regulations regarding service providers and their Subprocessors. Often it is a “must” to go through a long process to select and onboard any service providers (and their Subprocessors). So there will be a strong need for B2B customers to have at least the possibility to get a list of the involved subcontractors, as well as a chance and right to audit all Subprocessors (if wanted and feasible to accommodate for the CSP and if no third party independent audit/certification is already provided). Of course, this will be a question of the price model as well the software and solution provided by the CSP and the feasibility to conduct such audits, if they are repetitive (e.g. when each customer asks for the same verifications of the control environment): The more standard the product is/ the cheaper the services are, the less room is there for such individual requirements of the customers. Generally speaking, many CSPs respond to individual audit requests by presenting independent detailed third party audits / certifications as the Cloud Service is the same for each Consumer / SME and can hence be audited for each Consumer / SME in a generic fashion.

C. **Subcontracting – Risks and Benefits**

Generally, the notion of providing Cloud Services by using subcontractors in various constellations is likely to be immanent to most Cloud Computing Services for consumers and SME, in particular unpaid services. Only very unexperienced customers will think it plausible that one company/legal entity only provides the Cloud Service entirely. As detailed above, subcontracting in Cloud Computing can appear in various shapes and constellations. There are various risks involved in subcontracting, for both parties to a Cloud Service agreement, the customer and the CSP. However, at the same time, subcontracting also offers benefits, which must be closely considered.

I. **Risks**

1. **Role as Data Controller (Fulfilment of Responsibilities from a Data Protection Perspective)**

   In general, (exemptions might apply), where consumers process personal data for mere private/family purposes, the end customer (in particular SMEs) is the data controller who is responsible for compliance with data protection rules. The data controller must take all measures necessary to ensure the delivery of this protection in practice. Especially for subcontracting in Cloud Computing, it is of vital importance to deal with duties and responsibilities imposed by data protection legislation clearly and unambiguously. The data controller can only ensure effective control over its sub-processors throughout the subcontracting chain without responsibilities getting lost “on the way”, if it makes sure that it fulfills its obligations. However, in practice, with the involvement of non-EU/EEA subcontractors a “loss of controllership” seems unavoidable.

2. **Change of Role**

   In concluding a subcontracting contract, the CSP that has been offering a service to a customer automatically becomes a customer, demanding the supply of certain services from a third party. This change of role entails further obligations from a contractual as well as from a data protection perspective. Whereas from a contractual point of view the CSP is entitled to give instructions etc. to the Subprocessor,
from a data protection point of view the Controller retains its position as Controller and remains responsible for the admissibility of the processing. At the same time, the Processor (CSP) is not entitled to give instructions to the subcontractor. In practical terms, contracts typically provide for the obligation of the CSP to pass on any instruction to the Subprocessor as the Consumer / SME has no direct relationship to the Subprocessor or the CSP should directly contact the Subprocessor who may otherwise not be able to verify if the instruction is valid and legally permissible. Furthermore, conflicting instructions by several Consumers / SME might not be easy to accommodate if they changed the nature or scope of the Cloud Service itself (which is based on a multi-tenant architecture so that all customers receive the very same Cloud Services).

3. Responsibility

Subcontracting does not relieve CSPs and/or customers of their responsibilities. They remain responsible for fulfilling both – data protection requirements as well as contractual duties and obligations towards their data subjects and/or contractual partners (e.g. customers of the customer). They cannot transfer this responsibility to the subcontractor. However, in practice, it may be difficult for the CSP and/or the customers to fulfill all requirements this responsibility entails. Particularly if the Subprocessor is located outside the EEA, the parties should be aware of the additional hurdles to control the Subprocessor and the Cloud Service Provider should be asked to explain how it monitors, audits and controls the Subprocessor (e.g. through technical restrictions to access the Cloud Service or otherwise). It is questionable whether Consumers / SMEs de facto exercise the third party beneficiary clauses of the EU Model Clauses and if they could potentially intervene or circumvent the responsibilities designated by the contracting parties.

4. Transparency

If the CSP has agreed with the customer (or the Cloud Service Agreement includes such a provision) that the CSP may conclude contracts with subcontractors, then the CSP must always be in the position to name all subcontractors commissioned. Consequently, if the subcontractor contract allows for further subcontracting, the CSP must be able to fulfill this obligation as well. The CSP must thus always make sure to respect transparency towards the customer in all subcontracting contracts that may be concluded in a Cloud Service chain.

On the other hand, as a controller the customer must be able to know at all times – at least under German data protection law - , where the data is processed, by whom and under which circumstances, i.e. even in cases of subcontracting basic data protection rules must be fulfilled, before the execution of the subcontracting contract. The customer must thus always ensure that the Cloud Service agreement concluded with the CSP includes an obligation for the CSP to inform the customer about the identity of further Subprocessors, ideally in data protection terms, the customer will need to give its prior consent, before the CSP commissions a subcontractor.

5. Auditability of CSP (and Cloud Provider Chains)

Auditability is another aspect of transparency. The data controller is obliged to audit its processors who it entrusts with processing personal data. In order to be able to fulfill this obligation, the subcontracting contracts and the subcontracting chain must not only include extensive auditing rights but also provide for a clear procedure. In practice, conducting audits regarding the technical and organizational security measures taken at the subcontractor is unrealistic for consumers and SME, particularly in non-EU/EEA countries.

6. Security

Subcontracting chains, not necessarily long ones, are susceptible to security breaches. Without an adequate contractual basis, sufficient specification of security measures and ensuring that the security measures are indeed in place before the execution of the subcontracting contract, from a data protection point of view the risk of security breaches lies primarily in the controller’s sphere of responsibility (see e.g. data breach notification in Germany). Furthermore, if subcontractors are used, it is even more difficult with regard to the direct contractual partner (CSP) that the customer ensures that its data, which may include business or trade secrets is reliably erased from subcontractors’ servers after termination of the contract. The contracts with the subcontractors may not provide sufficient guarantees regarding security measures and their enforcement in practice.

7. Use of Subcontractors located in Third Countries

If a customer uses subcontractors located in non-EEA countries, it must ensure that they provide an adequate level of data protection. Some countries, e.g. Germany require a customer even to ascertain that
the measures the subcontractor claims to have taken are actually in place. Thus, although it may be particularly difficult to meet these requirements when using a subcontractor located in a country outside the EU/EEA, it is up to the CSP/customer to fulfill this obligation. It is obvious, that this is not only a difficult, but in many cases factually even an impossible task.

8. Liability
The CSP remains liable towards the end customers, even if it uses subcontractors to provide parts of the contractual services. Consequently, in case of a breach by a subcontractor, the CSP remains liable towards the end customers.

On the other hand the customer is liable for any breaches vis-à-vis its own customers. The subcontractors have no direct liability towards persons who are not their direct contractual partners. This applies both to liability from a data protection perspective as well as from a contractual perspective.

9. Monitoring
The data controller must not only choose the data processor by reviewing the technical and organizational security measures. From a data protection law perspective it is also required to monitor the data processor and thus to make sure that the data processor also applies the technical and organizational security measures it has committed to. In practice, especially for non-EU/EEA subcontractors it is impossible for CSPs and end customer to monitor the subcontractor’s compliance.

10. Termination of Subcontracting Agreement
Subcontracting agreements may be terminated ordinarily or extraordinarily, with or without notice. This may affect both the end customer and the CSP. The CSP must make sure a transition to another subcontractor is possible while making sure to fulfill its obligations towards the customer. For the end customer it is important to be sure that any data are returned and that copies are destroyed. If the subcontractor is located outside the EU/EEA, this may be complicated.

11. Insolvency of Providers
Insolvencies pose a serious risk for both CSPs and end customers. They will find themselves in the position that they will immediately need to find new subcontractors in order to fulfill their agreements towards their customers (storage space, provision of services etc.). In many cases, there will be no transition scheme and it may not even be ensured that all customer data can be retrieved.

12. Passing-on of claims
In the subcontracting relationship, the customer will most likely try to pass on any claims brought against him, which it considers caused by a failure or omission on the subcontractor’s side. To achieve this, the contracts between customers and subcontractors must clearly describe and specify the contractual basis of subcontracting (services, roles and responsibilities).

II. Benefits

1. Cost Efficiency
Cost efficiency is a strong benefit for both end customers and CSPs. An end customer is not required to reserve storage capacities, purchase services or infrastructure etc. which may be required for a certain limited period of time (e.g. at peak work times) or which are too expensive to purchase and maintain in their systems. For a CSP subcontracting is cost efficient, because it allows the provider - especially SMEs - to offer a range of services at a price it could not afford, if there were no subcontractors involved. Furthermore, the customer receives regular updates and upgrades of the Cloud Service that apply in a seamless fashion for the end user and are included in the subscription fees without additional license or maintenance fees.

2. Scalability
Scalability is another key benefit of Cloud Computing, both for CSPs and end customers. A CSP, especially an SME, is not able to provide unlimited services, i.e. in case its customers need to upscale, involving a subcontractor is a fast and easy solution. From the end customer’s perspective, the same is true: if it finds it needs to upscale, the typical questions regarding licenses, capacities, availability of infrastructure, applications etc. will not apply, because of the scalability of Cloud Services. Typically, this is only possible because the CSP has involved subcontractors.
3. Fast Response to Customers' Needs

A CSP is likely to cooperate with a number of subcontractors. This network allows especially SMEs with smaller capacities to respond quickly to their customer’s expectations, needs and requirements.

4. Shared Resources

In general, shared resources are a typical benefit of Cloud Computing but become even more prominent when viewed in connection with subcontracting. A CSP can offer a wider range of products and services to its customers, if it has concluded subcontracting contracts with other service providers.

5. Diversity of providers / no monopoly of international providers

Subcontracting allows smaller providers (SME) to provide services to large companies without the need to be in the position to provide a whole range of services by themselves. This leads to a wider diversity of providers on the market, the Cloud Computing business is not simply left to some few international providers with large capacities who are in all cases able to meet the needs of the market. Consequently, customers can choose and compare various providers and can decide on the one most suitable for their needs. A normal competition situation on the market favours customers.

D. Critical Links between End Customer Contract and Subcontractor Contract

CSPs usually subcontract a wide variety of functions to third parties (i.e. hosting, storage, processing, transmission, network security, etc.), and in most cases such subcontracting involves processing of or access to customer data. Most EU Member States’ legislation imposes an obligation on service providers to obtain the customer’s consent before entering into a subcontract for the performance of whole or part of the service. As an example, the Italian Civil Code e.g. (art. 1656) states that the contractor cannot subcontract the performance of a work or of a service, unless the customer has authorized it accordingly. Such permission is generally included in the Service Agreement. If an end user considers using cloud solutions, the end user should know and consider any subcontractors that the CSP relies on, or intends to rely on. A failure or issue at any point in the cloud “supply chain” could affect the service provided to the end user and could particularly affect its ability to access and recover its data.

I. Consistency of Contractual Provisions

Even in case of subcontracting the service provider remains responsible towards the customer for any part of the service entrusted to a subcontractor. In order to mitigate risks for the end customer (e.g. underperformance, inappropriate security measures with respect to service offering subscribed by end customer) it is crucial that the CSP imposes to its subcontractors the same obligations agreed between CSP and customer. Such back to back agreements need to be carefully verified with particular respect to some critical issues like the terms for prior notice in any event of suspension of the service or termination of the subcontract, for prior notification obligations in case of security breaches.

II. Description/Specification of Service

If the CSP uses subcontractors, customers should know what those subcontractors provide as a part of the whole Cloud Service. The more subcontractors are involved in the supply chain the higher is the risk that the end customers receive services that do not comply with the contractually envisaged characteristics and specifications.

III. Service Levels/Time Zone Differences

The CSP must verify the possibility for the subcontractor to guarantee the SLAs agreed between provider and customer. This means considering any aspect that may possibly impact on their respect, such as time zone differences, but also peculiar liability exemptions for SLAs, eventually qualified by subcontractor as “force majeure”.

1 For a comparative view see also the Draft Common Frame of Reference (DCFR) by the Study Group on a European Civil Code and the European Research Group on Existing EC Private Law of 1.1.2009
IV. Cooperation Duties/Active Involvement of the Customer

Cloud customers are often unaware of the responsibilities or activities assigned to them within the terms of the Service Agreement. When CSPs rely on third party suppliers to provide and support their cloud solutions, those third party suppliers may need to interact directly with the end customer and to access the technology solutions provided by the CSP in order e.g. to perform troubleshooting or problem analysis and resolution, which otherwise may not be timely provided.

V. Change Management/Change Request/ Data Protection Instructions of the Controller

In case of subcontracting of processing activities, the end customer has to give its prior authorization to the CSP for sub-processing. In case of sub-processing the end customer acting as Controller should be put in the position to provide to CSP subcontractors data protection instructions for processing. This may be difficult in case of a supply chain which involves many different players. This is due to the fact that the Controller, which in any case will be liable for the processing operation, may risk to lose control of the activities of each subcontractor in the provision of the service. This would very possibly happen if a change in the provision of a part of the service provided to end customer is agreed at CSP level. The Service Agreement should therefore include an obligation for CSPs to provide transparent and updated information about subcontractors involved in the provision of Cloud Services to end customers, thus allowing end customers to fulfill their obligations as Controllers, and to certain extent, some audit rights in order to be able to check the compliance with its instructions by CSP subcontractors.

VI. Subcontracting and IP

Although Cloud Computing contracts relate to the provision of services rather than to the supply of software to customers, the customer still needs the grant of appropriate software licenses to enable them to use the necessary software legally and correctly without the risk of copyright infringements. The CSP will not always own the intellectual property rights in the software that is the object of the Cloud Computing service. Where this is the case, as in case of subcontracting, the CSP will need to arrange for the right to sub-license the software to its customers, or for a direct license to be entered into between the customers and the relevant third-party licensor with service provider just managing the third party licenses. The subcontract agreement must include sound intellectual property rights warranties and indemnities in case of IPR infringement by end customers using software as part of the service, sufficiently broad to protect the CSP and its end customers in all jurisdictions in which they will use the software.

VII. Warranty and Liability

The CSP must guarantee that any third parties to which it subcontracts any service or processing activities will provide adequate warranties and an equivalent level of protection as agreed between the CSP and the customer, by ensuring to make necessary legal and operational arrangements to enforce this level of protection. Under data protection law the CSP must ensure that in case of sub-processing it can at all times demonstrate to the customer acting as Controller, that it has taken measures to provide this same level of protection and that a written agreement with the third party exists, which imposes the same obligations as agreed between the CSP and the customer.

VIII. Subcontracting and Antitrust Law (internal/external Subprocessors)

Subcontracting in cloud environment allows multiple players to offer their services; the development of a wide range of alternative Cloud Computing solutions that may involve small external or internal subcontractors in case of big CSP organizations, is changing the prevailing business model in ICT and is determining wide investments in innovation by the many players. Consequently, the development and success of cloud services is associated with providing innovative solutions rather than with the exploitation of “network effects” or barriers to entry. Such a number of players would probably share the market and play a role in the supply chain of cloud services, without the risk of excessive concentration. Therefore, even if on the one hand the presence of a large number of players in the supply chain of cloud services may lead to a lock-in effect, on the other hand in order to stay on the market it is primarily of interest for such players to develop solutions with a high degree of interoperability.

IX. Termination of the contract

In case of termination of subcontracting relationships, CSPs may not be in the position to assure continuity of service to the end customer. The end customer may risk losing access to and availability of its data. As the end
customer is the Controller, it may also find itself exposed to liability towards its own customers under data protection law. Prior notification and information about data location is of essence in order to manage the transfer and or deletion of the data processed by the subcontractor, considering that data may be stored and/or processed by subcontractors in high-risk jurisdictions. In such jurisdictions, by way of example, it may be subject to confiscation by forced entry.

E. Requirements from a Data Protection Law Perspective

I. Statutory Regulation

1. Directive 95/46/EC

Under Directive 95/46/EC processing of personal data is allowed only in the quality of “data controller” or in the quality of “data processor”. The Data Controller under Article 17 of the Directive may choose only processors “providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out and must ensure compliance with those measures”. Only the Data Controller may appoint a third party as Data Processor, so that the appointment of a Data Processor by another Data Processor is forbidden. This means that in case of subcontracting, subcontractors must be appointed as Data Processors directly by the Data Controller and may not be appointed by the main contractor (which is generally itself a processor).

2. Draft of a EU General Data Protection Regulation (EU Commission versus LIBE)

The proposed new EU data protection regime originally released by the European Commission on January 25, 2012, extends the scope of the EU data protection law to all foreign companies processing data of EU residents and provides for a harmonization of the data protection regulations throughout the EU. Some remarkable changes with respect to current legislation and relevant when referring to subcontracting are:

- the EU data protection regulation will also apply for all non-EU companies without any establishment in the EU, provided that the processing of data is directed at EU residents
- as a general rule, any processing of personal data will require providing clear and simple information to concerned individuals as well as obtaining specific and explicit consent by such individuals for the processing of their data (Opt-in), other than in cases in which the data protection regime explicitly allows the processing of personal data;
- the Regulation will make a safe transfer of data outside the EU (including the processing of data in clouds) easier if the parties involved commit to binding corporate rules (BCR).

- All companies will be obligated to notify EU data protection authorities as well as the individuals whose data are concerned by any breaches of data protection regulations or data leaks without undue delay.

3. Data Transfer Agreements (Controller to Processor) according to Member State Data Protection Legislation (Germany / Italy)

a. Sec. 11 German Federal Data Protection Act for non-public sector; Data Protection Acts of German States

b. Title VII (articles 42-45) Legislative Decree no. 196/2003 (“Code”)

The rules concerning cross-border data flows are set in Title VII (articles 42-45) of the Code.

In short, the Code provides for a free flow of personal data within the EU/EEA, while transfer of personal data to countries outside of the EU/EEA are allowed only on the ground of at least one of the following conditions:

- authorizations issued by the Garante (Italian Data Protection Authority), based on the official recognition by the European Commission that the foreign country ensures an adequate level of data protection;
- adoption of the standard contractual clauses provided by the EC;
- adoption of BCR for data transfers within the framework of companies all belonging to the same group;
- if the transfer is necessary for the performance of obligations resulting from a contract to which the data subject is a party;
other conditions, less frequently applicable in ordinary business circumstances, such as a specific consent of (all) data subjects, an obligation provided by a law, the necessity to safeguard a third party’s life, etc.

Regarding Subprocessors established outside the EU, we may distinguish two possible cases.

(1) Transfer from a Data Controller within the EU (data exporter) to a processor outside the EU (data importer) and onward to a Subprocessor outside the EU:
In this case, according to the European Commission’s decision no. 2010/87/EU and to the relevant Garante’s authorization no. 35/2010, all of the following requirements must be fulfilled:
- written consent of the data exporter to subcontracting;
- a written contract between the data importer and the Subprocessor;
- the Subprocessor’s commitment to process the data in compliance with the data exporter’s instructions;
- the Subprocessor must sign the same standard contractual clauses signed between data exporter and importer;
- the data importer must send to the data exporter a copy of the contract signed with the Subprocessor.

In any case, the data importer remains liable also for any failure of the Subprocessor. Furthermore, data exporters must keep a register of the existing subcontracts, updated at least annually.

(2) Transfer from a data controller within the EU (data exporter) to a processor within the EU (data importer) and onward to a third party (Subprocessor) outside of the EU.
In this case, according to the Working Paper no. 176, adopted by the Article 29 Working Party on July 12th, 2010 and to the decision issued by the Garante on November 15th, 2012, the Data Controller may, alternatively:
- sign the standard contractual clauses directly with the third party (which will sign them as data importer, not as sub-processor, and therefore shall be appointed as data processor);
- sign a specific mandate, in order to allow the Subprocessor to sign the standard contractual clauses on its behalf;
- sign with the Subprocessor an ad hoc contract, which the Garante must approve previously.

Furthermore, also in this case, the Data Controller must authorize subcontracting in writing. The Data Processor must send to the Controller a copy of the contract signed with the Subprocessor and data exporters must keep a register of the existing subcontracts, updated at least annually.

4. EU Model Clauses

The free flow of personal information is essential for the efficient conduct of almost any economic activity on an international basis and is almost “implied” in cloud computing services environment. The EU Model Clauses help addressing this need: by (voluntarily) incorporating the standard contractual clauses into a contract, personal data can flow from a Data Controller established in any of the EU/EEA member countries to a Data Controller or to Data Processors established in a country not ensuring an adequate level of data protection. The 2010 Controller to Processor Clauses have taken account of the expansion of processing activities and have envisaged the situation where there is further outsourcing of processing to Subprocessors, starting with introducing a definition of Subprocessors. This extends not just to an entity acting as a Subprocessor to the main processor (data importer) but to Subprocessors engaged by Subprocessors — so the requirements flow all the way down the supply chain. Under these regulations the Subprocessor agrees to process personal data in accordance with the Data Controller’s (i.e. data exporter’s) instructions, terms of the model clauses and the terms of the written subcontract. A data importer must not subcontract without the prior written consent of the data exporter and then only by way of a written agreement imposing the same obligations on the Subprocessor as the model clauses impose on the data importer. The data importer remains fully liable for the activities of its sub-processors. Under the new clauses, if the data importer has disappeared then the data subject can assert claims against the Subprocessor (unless any successor entity has taken on the entire legal obligations for either the data exporter or the data importer). However, the Subprocessor’s liability is limited to its own processing operations.
5. **BCR / BCR for Processors (Article 29 Working Group, WP 195, 204)**

BCR for Processors are meant to be a tool which should help frame international transfers of personal data that are originally processed by a Processor on behalf of an EU Controller and under its instructions, and that are subprocessed within the Processor’s organization. Therefore, BCR for Processors shall be annexed to the Processor contract, which is required by Art. 17 of EU Directive 95/46 and contains notably the instructions of the Controller signed between the external Controller and the Processor. BCR for Processors should be understood as adequate safeguards provided by the Processor to the Controller (Art. 26.2 of EU Directive 95/46) allowing the latter to comply with applicable EU data protection law. The Processor’s group entities shall commit to the principles contained in the BCR for Processors and shall be held liable vis-à-vis the Controller in case of breach of the BCR for Processors.

6. **Conclusions: CSP Chains; Transfer from Processor within the EU to Processor in Third Countries; loss of the Controller’s controllership**

Given the always-increasing sophistication of vendor services and outsourcing relationships it is increasingly difficult to draw a clear distinction between Data Controllers and Data Processors. CSP chains pose many issues with respect to protection of personal data and business sensitive data of end customers, which compliance with the legislative and regulatory framework cannot effectively address. The loss of the Controller’s controllership on data processing is one of the major and most difficult issues to tackle and exposes the Controller to high liabilities if it is not able to govern the purposes and means of processing.

II. **Interplay of Data Protection Law and Contract Law**

According to data protection law, only the Data Controller may appoint a third party as Data Processor, so that one Data Processor cannot appoint another Data Processor. The Data Controller must therefore directly appoint Subcontractors as Data Processors directly by the Data Controller, not by the main contractor. Liability for any wrongdoing committed by the provider and its subcontractors acting as processors under its instructions remains with the Data Controller.

Under contract law the provider remains fully responsible for any part of the service entrusted to a subcontractor and bears all responsibilities with respect to the service process itself and for the choice of its selected subcontractors which should be capable of performing the service or part of it as subcontracted. The CSP freedom to choose subcontractors if authorized by its customer, for the performance of which it retains all liabilities, may be difficult to combine with customer obligations and responsibilities acting as Data Controller giving instructions to CSP subcontractors acting as Data Processors.

A SME or a local authority might find it hard to negotiate appropriate terms for the management of “cloud-based” data; still, claiming that the client was unable to negotiate more stringent contractual terms or supervision mechanisms will not suffice to justify violations. Indeed, a client of cloud-based services can apply to other CSPs, who may afford more robust safeguards, especially concerning data protection. This means, though, that each customer needs to know the CSP subcontractors and needs to have a say about them, which may be very difficult to fit with CSPs providing standardized solutions to many customers, not able to adjust their supply chains according to single customer needs.
F. Specific Issues for Persons Subject to Professional Secrecy (e.g. Attorney Client Privilege)

I. Overview

Some natural or legal persons, e.g. lawyers, physicians, but also insurances, are bound by professional secrecy by some national legislations. In Germany, professional secrecy is even protected under criminal law and prevents the relevant professionals from letting other persons than specialized employed aids of these professionals take notice of the private secret. Sec. 203 Paragraph 1 of the German Criminal Code states the following: “Whosoever unlawfully discloses a secret of another, in particular, a secret which belongs to the sphere of personal privacy or a business or trade secret, which was confided to or otherwise made known to him in its capacity as a [...] 3. attorney, patent attorney, notary, defense counsel in statutorily regulated proceedings, certified public accountant, sworn auditor, tax consultant, tax agent, or organ or member of an organ of a law, patent law, accounting, auditing or tax consulting firm in the form of a company; [...] shall be liable to imprisonment not exceeding one year or a fine.” This provision very likely excludes IT outsourcing and IT services for lawyers. However, lawyers, physicians, social workers, etc. should not per se be excluded from using Cloud Services. Nevertheless, due to very strict national legislation the use of Cloud Services by these persons and entities can be difficult. In order not to exclude entire business branches from cloud computing, it is necessary to seek and implement a comprehensive legal solution.

II. Use of Cloud Services by Lawyers

1. Professional Obligations / Release from Confidentiality etc.

Lawyers are specifically obliged to maintain secrecy about their clients’ information they receive in the exercise of their profession. Only if their clients have released them from confidentiality, they may disclose such information to third parties. In Germany, the solution in practice is to inform the clients that they will be receiving communication, for which their lawyers cannot ensure to keep it completely confidential, due to technological reasons. It is then up to the client to object to communication by electronic means (e.g. e-mail) etc.

2. Challenges in Connection with the Use of Cloud Services (Criminal Sanctions, etc.)

In Germany, the obligation to maintain professional secrecy is even included in the Criminal Code, i.e. a breach can lead to criminal sanctions. In the light of the technological progress and the benefits derived from cloud computing (IT-infrastructure, mailing services etc.), it is difficult to argue that persons subject to professional secrecy should be excluded from the use of Cloud Services. This is especially true where in fact lawyers and/or physicians and other persons bound by professional secrecy (usually in small units) are already making use of these services (e.g. webmail services) and are thus risking criminal sanctions.

For this particular problem, encryption alone is not a solution: applying encryption would render IT outsourcing compliant with requirements of data protection. However, making use of such solutions would not solve the problem of factual violation of professional secrecy. Consequently, persons bound by professional secrecy find themselves in a dilemma, which they cannot presently solve by technology alone.
Annex 1
Selected Clauses from the Major Cloud Service Providers Regulating Subcontracting in Cloud Computing

I. Amazon Web Services: No provisions

II. Citrix: No provisions

III. Dropbox: No provisions

IV. Google: No provisions

V. Joyent: No provisions

VI. Microsoft Office 365: No provisions

VII. Netsuite: No provisions

VIII. Oracle Cloud: No specific provisions on modalities of Subcontracting, but Oracle seems to assume that it will be using subcontractors for providing services: Clause 23.1, Other

“23.1 […] Oracle is not liable for, bound by, or responsible for any problems with the Services arising due to, any acts of any such business partner or third party, unless the business partner or third party is providing Services as an Oracle subcontractor on an engagement ordered under this Agreement and, if so, then only to the same extent as Oracle would be responsible for Oracle resources under this Agreement.” (Oracle SaaS-Online Cloud Services Agreement - UK Version, effective from 1 December 2012)

IX. Rackspace.com: Clause 27, Assignment/Subcontractors

“27. ASSIGNMENT/SUBCONTRACTORS
You may not assign the Agreement without Rackspace’s prior written consent. We may assign the Agreement in whole or in part to an Affiliate with sufficient financial standing in order to meet its obligations under this Agreement or as part of a corporate reorganization or a sale of our business, and we may transfer your Confidential Information as part of any such transaction. Rackspace may use third party service providers to perform all or any part of the Services, but Rackspace remains responsible to you under this Agreement for work performed by its third party service providers to the same extent as if Rackspace performed the Services itself.” (Cloud Terms of Service, dated February 14, 2014)
Available at: http://www.rackspace.com/information/legal/cloud/tos

X. Salesforce: No provisions

XI. SAP (B2B only – applies to the majority of SAP Cloud Services):

Art. 12.10: “SAP may in its sole discretion sub-contract parts of the Service to third-parties.” (General Terms and Conditions)

Subprocessors (Art. 5): “Customer hereby authorizes SAP (also in accordance with Clause 11 paragraph 1 of the Standard Contractual Clauses) to engage subcontractors for the processing of personal data (each a “Subprocessor”) to the extent necessary for fulfilling its contractual obligations under the Agreement as long as SAP remains responsible for any acts or omissions of its Subprocessors in the same manner as for its own acts and omissions hereunder. SAP shall pass on to Subprocessors SAP’s obligation as data processor vis-à-vis Customer as set out in this Policy and obligate Subprocessors to obey all relevant data protection rules. SAP will inform Customer upon its request by email or through a web site accessible to Customer about the name, address and role of each Subprocessor. SAP may remove or appoint suitable and reliable Subprocessors at its own discretion. SAP will inform Customer by email or otherwise in advance of any changes to the list of Subprocessors. If Customer has a legitimate reason to object to SAP’s use of a Subprocessor Customer shall notify SAP thereof in writing within thirty (30) days after receipt of SAP’s notice. If Customer does not object during such time period the new Subprocessor(s) shall be deemed accepted. If Customer objects to the use of the Subprocessor concerned SAP shall have the right to either
provide the Service without such Subprocessor or to terminate the Agreement with thirty (30) days prior written notice. In any event, SAP shall ensure that each Subprocessor adheres to an adequate level of data protection by law or contract not materially less protective than the obligations applicable to SAP under the Agreement. In case that such Subprocessor is located outside the EU, SAP shall provide for a level of data protection deemed adequate under EU data protection regulations.” (Data Privacy and Security Policy, currently in the version from February 2013)

XII. Savvis: Clause 19, Assignment/Subcontractors

“19. ASSIGNMENT/SUBCONTRACTORS
You may not assign the Agreement without Savvis’s prior written consent. We may assign the Agreement in whole or in part to an Affiliate or as part of a corporate reorganization or a sale of our business, and we may transfer your Confidential Information as part of any such transaction. Savvis may use third party service providers to perform all or any part of the Services, but Savvis remains responsible to you under this Agreement for work performed by its third party service providers to the same extent as if Savvis performed the Services itself.” (Terms and Conditions, dated November 8, 2012)
Available at: https://www.savvisdirect.com/terms-conditions

XIII. Softlayer (IBM): Clause 19.5, Assignment/Subcontractors

“19.5 Assignment/Subcontractors. Customer may not assign the MSA or Customer rights and/or delegate Customer obligations under the MSA without SoftLayer’s prior written consent. Any assignment or transfer of the MSA by Customer in violation of this section will be void. SoftLayer may assign the MSA to (i) its Affiliates and (ii) any entity as a result of a merger or sale of all or substantially all of the assets of SoftLayer to such entity and such entity agrees in writing to be bound by the terms of the MSA. This MSA will be binding on and inure to the benefit of Customer’s and SoftLayer’s respective permitted successors and permitted assigns. However, SoftLayer may use Third Parties or Affiliates to provide all or part of the Services. This provision does not apply to the Third Party Services which are governed by separate agreements.” (Master Services Agreement, dated October 2013) Available at: http://cdn.softlayer.com/SoftLayer_MSA.pdf

XIV. Terremark (Verizon): No provisions

XV. Zoho: No provisions
Annex 2
Excerpts from Selected Opinions and Working Papers on Subcontracting in Cloud Computing
(Germany, Italy and International)

I. Germany


„3.1 Verantwortlichkeit des Cloud-Anwenders

3.2 Kontrolle der Cloud-Anbieter

3.3 Betroffenenrechte
Der Cloud-Anwender bleibt als Auftraggeber nach § 11 Abs. 1 BDSG zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet, wobei ihm auch die Verpflichtung obliegt, personenbezogene Daten nach den §§ 34, 35 BDSG zu berichten, zu löschen, zu sperren und auf Verlangen des Betroffenen Auskünfte vor allem zu den zu seiner Person gespeicherten Daten und zur Herkunft der Daten zu erteilen. Da der Cloud-Anwender nur einen sehr eingeschränkten administrativen, operativen und kontrollierenden Zugriff auf die Infrastruktur des Cloud Computing hat, sollte er gegenüber dem Cloud-Anbieter vertragsstrafensbewehrte Weisungsrechte festlegen, die eine Erfüllung der Betroffenenrechte gewährleisten und diesem zusätzlich die Verpflichtung auferlegen, gegenüber Unter-Anbietern dieselben Rechte einzuräumen. Weiterhin können zur Durchsetzung der Betroffenenrechte technische Maßnahmen ergriffen werden (Kapitel 4).

[...]

3.4.2 Außereuropäischer Raum
Erfolgen die Datenverarbeitungen allerdings außerhalb der EU und des EWR, indem die Cloud-Anbieter und/oder Unter-Anbieter eine Datenverarbeitung in Drittstaaten vornehmen, so gelten die besonderen Anforderungen der §§ 4b, 4c BDSG für den Drittstaatentransfer. Falls in dem Drittstaat kein angemessen Datenschutzniveau besteht (Fn. 19), müssen daher durch den Cloud-Anwender als verantwortliche Stelle ausreichende Garantien zum Schutz der allgemeinen Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorgewiesen werden. Die Garantien können sich aus Standardvertragsklauseln oder u. U. aus Binding Corporate Rules ergeben (Fn. 20).
In jedem Fall ist ein besonderes Augenmerk auf die Festlegung eines technischen und organisatorischen Datenschutzes zu legen (Kapitel 4).

Im Rahmen des Datentransfers mit Drittstaaten erlangen die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG vom 05.02.2010 (Fn. 21) an Bedeutung. Demnach agiert der Cloud-Anwender als verantwortliche Stelle und Datenexporteur, der Cloud-Anbieter hingegen als Datenimporteur, sofern er in einem Drittstaat ansässig ist. (Fn. 22)

Gibt der im Drittstaat ansässige Cloud-Anbieter Daten an einen Unter-Anbieter, der ebenfalls seinen Sitz im außereuropäischen Raum hat, so wird Ersterer als Übermittler mitverantwortlich für die Rechtmäßigkeit der Datenübermittlung und -verarbeitung. Gleichwohl verbleibt eine Verantwortlichkeit des Cloud-Anwenders. Der Cloud-Anwender bleibt in jedem Fall haftungsrechtlich für sämtliche Schäden verantwortlich, die der Cloud-Anbieter oder Unter-Anbieter den Betroffenen zufügen.“


„9. Mindestanforderung Auftragsdatenverarbeitung
Gemäß § 11 Abs. 2 S. 1 ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Dies gilt nicht nur für den Cloud-Anbieter als erster Auftragnehmer, sondern auch für die Ressourcenanbieter als Unterauftragnehmer i.S.v. § 11 Abs. 2 Nr. 6 BDSG. Der Auftraggeber hat sich nach § 11 Abs. 2 S. 4 BDSG vor dem Beginn der Verarbeitung insofern zu vergewissern. Dies ist dem Cloud-Nutzer nur möglich, wenn er sämtliche an der Verarbeitung beteiligten Stellen kennt. Da es ihm faktisch nicht selbst möglich ist, die Zuverlässigkeit sämtlicher Cloud-Teilnehmer und die dortige Datensicherheit zu überprüfen, muss er sich auf externe Prüfungen verlassen (können). In einer Selbstzertifizierung kann keine zuverlässige Prüfung gesehen werden. Mindestvoraussetzungen sind, dass eine externe Überprüfung durch eine unabhängige Stelle erfolgt, die einen Prüfbericht vorlegt, der vom Cloud-Nutzer kontrolliert werden kann. Wegen der Vielzahl der möglicherweise vorhandenen Cloud-Beteiligten muss der Nutzer angezeigt bekommen, bei welchen Anbietern derzeit eine Verarbeitung konkret erfolgt. Anderenfalls kann der Nutzer seinen Aufgaben als verantwortliche Stelle nicht nachkommen.

Es sollte sich von selbst verstehen, dass bei der Benennung der technisch-organisatorischen Maßnahmen nicht nur die abstrakte Methode oder das Schutzziel benannt werden müssen, sondern das konkret genutzte Sicherungsmittel (§ 11 Abs. 2 S. 2 Nr. 3). Dies gilt auch für die Kontrollmaßnahmen nach § 11 Abs. 2 Nr. 5, die vom Cloud-Anbieter gegenüber den Ressourcenanbietern durchgeführt werden müssen. Dazu gehört, dass die Anbieter vertraglich verpflichtet werden müssen, spezielle Überprüfungen auf ungewöhnliche oder unzulässige Aktivitäten hin zuzulassen und tatsächlich durchzuführen. Auf Initiative des Nutzers muss die eine konkrete Verarbeitungskontrolle möglich sein, also ein Zugriff auf die jeweiligen Protokolldaten.“

3. BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., Cloud Computing – Was Entscheider wissen müssen, 2010

„2.2.3 Ein Vertragspartner – Cloud Provider als Generalunternehmer

Die Vorteile dieser Konstellation liegen aus rechtlicher Sicht darin, dass es trotz weitgehender Flexibilität und den damit verbundenen wirtschaftlichen Vorteilen aus Kundensicht bei einem Vertragspartner bleibt, der für die Leistungserbringung in Gänze verantwortlich ist. Auch in praktischer Hinsicht hat der Kunde hier im Idealfall nur einen Ansprechpartner, was die
Abwicklung deutlich vereinfacht und entsprechendes Know-how auf Kundenseite entbehrlich macht. Allerdings muss aus Kundensicht darauf geachtet werden, dass der Anbieter notwendige vertragliche Verpflichtungen (z. B. in datenschutzrechtlicher Hinsicht) an seine Subunternehmer weitergibt und der Kunde die für ihn notwendigen Informationen und Bestätigungen hierüber erhält.

[...]  

2.10 Vertragsbeziehungen und Subunternehmer  


Der Netzbetreiber (Provider) stellt Kunden einen Zugang zu einem Netz (in der Regel dem Internet) zur Nutzung von Cloud-Computing-Leistungen bereit.

Kunden von Cloud-Computing-Leistungen können drei Gruppen zugeordnet werden:
- Software-(SW-)Nutzung im Rahmen von SaaS,
- Nutzung einer Entwicklungs- oder Betriebs-Plattform im Rahmen von PaaS,
- Rechenzentrums-(RZ-)Nutzung im Rahmen von IaaS.

Der Software-Anbieter liefert dem SaaS-Anbieter die Software zur Bereitstellung von SaaS, sofern der SaaS-Anbieter nicht selber Hersteller der Software ist.


Der PaaS-Anbieter kann zwei unterschiedliche „Systeme“ bereitstellen:
- ein „Laufzeitsystem“ für den SaaS-Betrieb (z.B. Verwaltung der Zugangsdaten und Ermittlung von Abrechnungsdaten),

Der IaaS-Anbieter stellt RZ-(Infrastruktur-)Leistungen bereit.

[...]  

Die Vertragsbeziehungen und Konstellationen können bei Cloud Computing also durchaus vielgestaltig sein. Von besonderer Bedeutung ist es dabei für die Beteiligten, auf konsistente und durchgängige Vereinbarungsinhalte zu achten, die für alle Glieder einer Vertragskette gelten sollen.

3.6.3 Einbindung eines Subunternehmers  
Die Einbindung eines Subunternehmers (im Ausland) ist wahrscheinlich, wenn Data-Center im Ausland genutzt werden. Die praktische Frage aber bleibt – wer kontrolliert den Subunternehmer? Empfehlenswert, aber nicht unbedingt preisgünstig, ist eine direkte Auditierung der Systeme und deren Sicherheitsvorkehrungen und Logs des Anbieters und Auftragnehmers, was vor allem im Ausland auch durch Dritte bewerkstelligt werden kann.

Die European Network and Security Agency (ENISA) bringt in ihrer Risikobewertung ebenfalls den hohen Risikograd beim unbedachten Cloud Computing zum Ausdruck (Fn. 33). Reputationsverlust, Kundenvertrauen, sensible oder kritische Personaldaten und Serviceleistungen können als Firmen-Assets betroffen werden.

Die verantwortliche Stelle, die sich der Subunternehmer bzw. einer Kette von Subunternehmern bedient, bleibt immer für die Verarbeitung in der Haftung und kann sich nicht mit Nichtwissen exkulpieren oder die Haftung abbedingen.

Das gilt auch, wenn die verantwortliche Stelle / unmittelbarer Vertragspartner des Auftraggebers Datenlecks nicht an den Auftraggeber weitermeldet. Mit zunehmender Zahl der eingebundenen Cloud-Betreiber steigt demgemäß das Risiko, die Kontrolle über die

„10 Sicherheitsprüfung und -nachweis
Nutzt ein CSP Subunternehmen zur Erbringung seiner Services, so entlässt ihn dies nicht von der Verpflichtung, die Sicherheit dieser Dienste zu überprüfen, da der CSP gegenüber seinen Kunden für die Gesamtsicherheit seines Angebots verantwortlich und dies nicht auf Subunternehmer übertragen kann. In einem solchen Fall muss der CSP die erforderlichen Nachweise aller notwendigen Sicherheitsprüfungen von seinen Subunternehmern einfordern. Generell sollten durchgeführte Sicherheitsprüfungen so dokumentiert werden, dass es möglich ist, diese bei Bedarf an seine Kunden weitergeben zu können, sowohl die Nachweise beim CSP selber als auch bei dessen Subunternehmen.

[...]”

**12 Vertragsgestaltung**

Viele Anbieter von SaaS betreiben keine eigene Infrastruktur, sondern nutzen wiederum PaaS- oder IaaS-Angebote anderer CSPs. In solchen Fällen sind die für die Erbringung der Cloud Services wichtigen Subunternehmer gegenüber den Kunden offenzulegen und diesen die erforderlichen Informationen zur Verfügung zu stellen.

**12.2 Service Level Agreement (SLA)**
Setzt ein CSP Subunternehmer zur Erbringung der von ihm angebotenen Services ein (z. B. wenn ein SaaS-Anbieter IaaS von einem Dritten nutzt), so kann vom CSP aus Vertrauen geschaffen werden, indem den Cloud-Nutzern die relevanten Aussagen zur Informationssicherheit und zur Dienstgüte aus den SLAs mit Drittanbietern offen gelegt werden.”

II. Italy

*Guidelines on Cloud Computing entitled 'Cloud Computing - How to Protect the Data from Not Falling from the Clouds', published by Italian Data Protection Authority (Garante) on 24th May 2012.*

(http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906139)

III. International

1. **Article 29 Data Protection Working Group, Opinion 05/2012 on Cloud Computing, 1.7.2012**

“3.3.2 Subcontractors
Cloud computing services may entail the involvement of a number of contracted parties who act as processors. It is also common for processors to subcontract additional sub-processors which then gain access to personal data. If processors subcontract services out to sub-processors, they are obliged to make this information available to the client, detailing the type of service subcontracted, the characteristics of current or potential sub-contractors and guarantees that these entities offer to the provider of cloud computing services to comply with Directive 95/46/EC.

All the relevant obligations must therefore apply also to the sub-processors through contracts between the cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider. In its Opinion 1/2010 on the concepts of "controller" and "processor", the Article 29 Working Party referred to the multiplicity of processors in cases in which processors may have a direct relationship with the controller or operate as subcontractors where the processors outsource part of the processing work they had been tasked with. “Nothing in the Directive prevents that on account of organizational requirements, several entities may be designated as processors or (sub-)processors also by subdividing the relevant tasks. However, all of them are to abide by the instructions given by
the controller in carrying out the processing.” (Fn. 13).

In such scenarios, the obligations and responsibilities deriving from data protection legislation should be set out clearly and not dispersed throughout the chain of outsourcing or subcontracting, in order to ensure effective control over and allocate clear responsibility for processing activities.

A possible model of assurances that can be used to clarify the duties and obligations of processors when they subcontract data processing was first introduced by the Commission Decision of 5 February 2010 on the standard contractual clauses for the transfer of personal data to processors established in third countries (Fn. 14). In this model subcontracting is permitted only with the prior written consent of the controller and with a written agreement imposing the same obligations on the sub-processor as are imposed on the processor. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the processor shall remain fully liable to the controller for the performance of the sub-processor’s obligations under such agreement. A provision of this kind could be used in any contractual clauses between a controller and a Cloud Service provider, where the latter intends to provide services through subcontracting, to assure required guarantees for the sub-processing.

A similar solution regarding assurances in the course of sub-processing has been proposed recently by the Commission in the proposal for a General Data Protection Regulation (Fn. 15). The acts of a processor must be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that, among other requirements, the processor shall enlist another processor only with the prior permission of the controller (Article 26(2) of the proposal).

In the view of the WP29, the processor can subcontract its activities only on the basis of the consent of the controller, which may be generally given at the beginning of the service (Fn. 16) with a clear duty for the processor to inform the controller of any intended changes concerning the addition or replacement of subcontractors with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned. In addition, a contract should be signed between cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider. The controller should be able to avail of contractual recourse possibilities in case of breaches of contracts caused by the sub-processors. This could be arranged by ensuring that the processor is directly liable toward the controller for any breaches caused by any sub-processors it has enlisted, or through the creation of third party beneficiary right for the benefit of the controller in the contracts signed between the processor and the sub-processors or by the fact that those contracts will be signed on behalf of the data controller, making this later a party to the contract.

[...]

**4.1 Guidelines for clients and providers of cloud computing services**

Subcontracting safeguards: Provisions for subcontractors should be provided for in any contract between the cloud provider and cloud clients. The contract should specify that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned. The cloud provider should sign a contract with each subcontractor reflecting the stipulations of its contract with the cloud client; the client should ensure that it has contractual recourse possibilities in case of contractual breaches by the provider’s sub-contractors (see 3.3.2);

Compliance with fundamental data protection principles:

- Transparency (see 3.4.1.1): CSP should inform cloud clients about all (data protection) relevant aspects of their services during contract negotiations; in particular, clients should be informed about all subcontractors contributing to the provision of the respective Cloud Service and all locations in which data may be stored or processed by the cloud provider and/or its subcontractors (notably, if some or all locations are outside of the European Economic Area (EEA)); the client should be provided with meaningful information about technical and organisational measures implemented by the provider; the client should as a matter of good practice
inform data subjects about the cloud provider and all subcontractors (if any) as well as about locations in which data may be stored or processed by the cloud provider and/or its subcontractors;

- **Purpose specification and limitation (3.4.1.2):** the client should ensure compliance with purpose specification and limitation principles and ensure that no data is processed for further purposes by the provider or any subcontractors. Commitments in this respect should be captured in the appropriate contractual measures (including technical and organisational safeguards);

- **Data retention (3.4.1.3):** the client is responsible for ensuring that personal data are erased (by the provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes; secure erasure mechanisms (destruction, demagnetisation, overwriting) should be provided for contractually;

**Contractual safeguards (see 3.4.2, 3.4.3 and 3.5):**

- In general: the contract with the provider (and the ones to be stipulated between provider and sub-contractors) should afford sufficient guarantees in terms of technical security and organizational measures (under Article 17(2) of the directive) and should be in writing or in another equivalent form. The contract should detail the client’s instructions to the provider including subject and time frame of the service, objective and measurable service levels and the relevant penalties (financial or otherwise); it should specify the security measures to be complied with as a function of the risks of the processing and the nature of the data, in line with the requirements made below and subject to more stringent measures as envisaged under the client’s national law; if CSPs aim at making use of standard contractual terms, they should ensure that these terms comply with data protection requirements (see 3.4.2); in particular technical and organisational measures that have been implemented by the provider should be specified in the respective terms;

- **Disclosure of data to third parties:** this should be regulated only via the contract, which should include an obligation for the provider to name all its sub-contractors – e.g. in a public digital register – and ensure access to information for the client of any changes in order to enable him to object to those changes or terminate the contract; the contract should also require the provider to notify any legally binding request for disclosure of the personal data by a law enforcement authority, unless such disclosure is otherwise prohibited; the client should warrant that the provider will reject any non-legally binding requests for disclosure; “


“16. Prior to the use of CC, the controller should perform a risk assessment based on insight into the specific conditions and circumstances under which personal data will be processed by the Cloud Service provider and its subcontractors, if any. The risk assessment should include all of the locations at which personal data are processed or stored. If the Cloud Service provider uses subcontractors for parts of the processing, the risk assessment should also include all locations used by the subcontractors.

17. The controller should regularly review and update the risk assessment as long as personal data are processed by the Cloud Service provider.

[...]

19. The controller should consider whether it is necessary to secure access to at least one usable copy of data outside of the Cloud Service provider’s (and its subcontractors’) control, reach or influence. If this is deemed necessary, the copy should be accessible and usable by the controller independently of the Cloud Service provider’s and its subcontractors’ participation.”


“83. Furthermore, there are currently no standard contractual clauses developed for the purpose of governing the transfers of data from processors based in the EU to processors located outside the EU. This is a significant gap in particular in the context of cloud computing services, which would deserve undertaking additional work in order to put forward an appropriate new set of clauses.”

“The following table summarises the three possibilities in terms of negotiating contracts and agreements between the customer and the cloud provider.

<table>
<thead>
<tr>
<th>CLOUD PROVIDER</th>
<th>CUSTOMER</th>
</tr>
</thead>
<tbody>
<tr>
<td>A) Large company – strong ability to negotiate contract clauses</td>
<td>SME – Weak or lacking ability to negotiate contract clauses</td>
</tr>
<tr>
<td>B) Both the customer and the provider have the ability to negotiate contract clauses</td>
<td></td>
</tr>
<tr>
<td>C) SME – Weak ability to negotiate contract clauses</td>
<td>Large company or public administration - may negotiate contract clauses</td>
</tr>
</tbody>
</table>

Depending on the particular case (whether it is A, B or C), the way to tackle the issues identified in subsection I may differ significantly.

5. **Outsourcing services and changes in control**

**Defining the issues**

5.1 The agreement between the company and the cloud provider is likely to be defined as a contract intuitu personae. An intuitu personae contract is one in which a party chooses to contract with a company based on qualities that are unique to the company. For example, a customer may choose a particular cloud provider because of the conditions it offers, its reputation or professionalism, or its technical skills. As a result, the customer may be reluctant to see the cloud provider outsource all or part of the services to be provided to the customer.

5.2 The control of the cloud provider may also change and, as a result, the terms and conditions of the services provided by the cloud provider may change, too.

**Dealing with the issues**

5.3 In case A, we recommend that the customer determine whether services will be outsourced by the CSPS and whether the cloud provider issues some guarantees or warranties relating to the performance of the services outsourced. However, we do not recommend that the customer look to be able to restrict the outsourcing of services by the cloud provider. We also recommend that the contract be reviewed to determine how the cloud provider will communicate changes in control to the customer. The customer may also want to consider whether the contract includes the right to terminate the contract if a change in control occurs.

5.4 In cases B and C, the customer may choose to require that the outsourcing of services by the cloud provider be subject to the customer’s prior authorisation. To make this decision, the customer will need to be informed about the type of services that the cloud provider intends to outsource and the identity of the company to whom these will be outsourced. Even if the customer agrees to the outsourcing, it may want the cloud provider to issue some guarantees or warranties relating to the performance of the services outsourced. By the same line of reasoning, the customer may also want to have the chance to approve a change of control, or to terminate or renegotiate the contract in case of a change in the control of the cloud provider. Such options may be carefully specified in the contract between the company and the cloud provider by means of a ‘third-party outsourcing’ clause, a ‘warranties and indemnification’ clause, a ‘change in control’ clause, or a ‘termination of agreement’ clause – again depending on the bargaining power of the parties.

**Conclusions**

All the contractual clauses from section 1 to section 3 may be suitable for standardisation, except the relevant penalties, which depends on the parties’ bargaining power. Whereas the inner content of the contractual clauses in sections 4 and 5 depends itself on the bargaining power of the parties, they are less suitable for standardisation.”
Detailed further Questions

1. What is an effective and meaningful contractual and technical & organizational set up to foster the legitimate data flow / processing for the purpose of providing Cloud Services?

2. Do you generally distinguish between subcontractors with potential access to personal data ("Subprocessors") and those without potential access to personal data ("Subcontractors") and if so what additional pre-cautions would you require for Subprocessors?

3. What practical approaches could make it easy for Consumers / SME to assess the risks and benefits of a Cloud Service that makes use of certain categories of subcontractors (e.g. Subprocessors accessing personal data and/or being located outside of the EEA)?

4. Under what circumstances could it be required or advisable to insist on a direct contract between a Consumer / SME and a subcontractor (in the sense of a Subcontractor) and what role should the Cloud Service Provider (CSP) play in such a set up? Is it reasonable to request a CSP to absorb all obligations and liabilities also in case the Consumer / SME enters into a direct contract (for data processing purposes)?

5. Within today’s corporate structures with many global group companies (with corporate governance and data protection controls) should there be a “privilege of affiliates” providing or receiving Cloud Services and if so what parameters or conditions may have to apply?

6. What are practical examples to “control” or “monitor” multi-tiered sub-processing relationships and what limits may have to apply to protect reasonable interests of Consumers / SME? Is it, for example, reasonable to require the Cloud Service Provider to act as the sole control agent to subcontract and prohibit various levels of sub-processing? Are there technical controls or legal/contractual means available to ensure a controlled access to personal data in order to determine easily who has processed personal data at any given time?

7. Should it be sufficient for Cloud Service Providers to comply with a standard set of contractual and technical security standards regardless of their place of incorporation (within the EU or outside the EU)? How could a discrimination of EU based Cloud Service Providers be best eliminated?

8. Considering the parties agree that a Consumer / SME can object to a new Subprocessor used by a Cloud Service Provider (e.g. for Subprocessors located outside of the EEA/"safe countries"), and a Cloud Service Provider is unable to provide special treatment of such objecting Consumer / SME. Should the termination of the Cloud service agreement by the Cloud Service Provider be subject to certain conditions/parameters or should the parties freely agree on the ability to terminate the agreement? Is there a difference between paid/free Cloud Services?

9. If the parties agree to include a general permission in the contract that allows a Cloud Service Provider to change its Subprocessors used - how should this list be updated if subcontractors change: By informing each contracting partner individually? By publishing the changes on a website?

10. How can a Consumer / SME entrust the Cloud Service Provider to act as its “ambassador / control agent” to exercise certain data protection controls directly vis-à-vis the Subprocessor? Is it required or even beneficial to a Consumer / SME to be asked to enforce its rights directly against a non EEA based Subprocessor (through third party beneficiary rights in EU Model Clauses) or should the Cloud Service Provider “own” the contract with its Subprocessors while the Consumer / SME should take direct recourse always to the Cloud Service Provider?