EUROPEAN COMMISSION
Information Society and Media Directorate-General

Converged Networks and Services
Software & Service Architectures and Infrastructures

Brussels, 5th December 2011

Cloud Computing: Public Consultation Report

Responses Received

A public consultation on cloud computing in Europe was opened on 16 May and ran until 31 August 2011. There were 538 responses. The largest single group of respondents claimed to represent companies (230 from 538). The second largest group were individuals (182). The remainder were public administrations (33), academics (42) or "other" (51).

Analysis of responses

All respondent groups agreed that **rights and responsibilities are unclear** in cross-border situations. This view was supported by 135 companies, 122 individuals, 25 administrations, 30 academics and 31 others i.e. a total of 343 from 538, or 63%. Typical, illustrative replies include the following:

> *"IT service providers within the public services domain ….. widely lack the ability of defining clear SLAs with their (public service) customers.";*
>
> *"The rights and responsibilities surrounding healthcare data are unclear, including data ownership, responsibility for securing data and data governance.";*
>
> *"In the Cloud services we are using the terms of service which describes the rights and responsibilities of both parties. What has to be clear especially for the user is that the cloud provider cannot take all responsibility for the user. For example, the user has to think about business continuity also when using cloud services.";*
>
> *"It is clear that most SLA contracts are nonsense considering exception Laws and force-majeure. End-users want reliability and privacy and request us to provide it. But exception laws kill privacy or trade secret. Force-majeure kills responsibility….";*
>
> *"We use it but we have no idea, where to find the right info to (sic) the responsibilities."*

The **general lack of certainty in the legal framework** is also confirmed by the responses to the question "Is liability clear in cross-border situations?", to which all respondent groups overwhelmingly agreed that liability in cross-border situations is unclear. This view was supported by 90% of the respondents and there were very small variations among the different respondent groups (minimum of 87.5% for individuals and maximum of 95% for academics). It is interesting that liability is also unclear for 90% of the respondent companies since, unless they are particularly small, they should have easier access to legal advice. The question was answered by 496 of the 538 total respondents (92%) showing that it is an important area of concern for them. The analysis of the detailed answers indicates that many different aspects influence this lack of clarity:

First, many respondents just do not know. As expressed by one of them:

> '*Don't even know where to start looking for that type of information*'.

Many answers of this type came from individuals. Typical statements from respondents are:

> '*Industry doesn't inform users sufficiently*'. '*It's never listed clearly*'. '*Providers have no interest in letting their potential users know what the actual risks are*'.

Secondly, among those respondents that understand the general liability principles, there is still lack of clarity due to the inherent complexity of the problem. Liability is set by the contract signed between user and provider, but there are also specific aspects that have to follow existing rules and regulations (e.g. data protection) and these vary from country to country. The need of harmonising the different legislations, both within the EU and at international level, is also a widely shared opinion:

> *"There is a need for some basic international agreement on liability of providers providing services outside their territory."*

A last factor that increases complexity is that the applicability of laws depends on the type of legal issue, since for each type of issue (e.g. contract, criminal law, data protection, torts etc.) the jurisdiction may differ. One respondent stated:

> '*For data protection issues, the general rule is that the laws of the country where the data controller is based [apply]. For contractual disputes, Rome I* [593/2008] *is relevant. It states that, subject to exceptions, a court should apply the law chosen by the parties. Where torts are the issue e.g. libel, negligent advice, infringement of confidential information etc. the decision of which law to apply will be decided by referring to Rome II* [864/2007]. *Rome II states that, subject to exceptions, the applicable law is the law of the country in which the damage occurs, irrespective of where the events giving rise to the damage occurred, or where the indirect consequences of that event occur*.'

As expressed by one of the respondents: '*Vous posez vous même la question ... cela n'a pas l'air d'être clair pour vous non plus!* '[1].

Half the companies claimed to be **relatively clear (compared with individuals) about which jurisdiction applied** to their cloud operations. Affirming that they knew which jurisdiction applied to their cloud operations were 99 companies; while 102 did not know. The picture is somewhat **different for individuals** where only about one-third of respondents claim to know (60 versus 112). A typical reply among those who were unclear is:

> *"… rights and responsibilities can hardly be clarified in international data transfers through private contracts if it is unclear which jurisdiction applies. While the applicable laws can be defined, to a certain extent in the respective services agreement with the provider, there can also be mandatory laws which cannot be derogated by contractual agreement…";*
>
> *"Especially when providing services to customers in multiple jurisdictions, it is a significant burden to understand and comply with all laws and regulations."*

[1] As you yourself ask the question, it seems that the issue is not clear to you either.

Considering this level of uncertainty, 135 individuals consequently feel that **guidelines and checklists** on **model terms for contracts** would be useful (compared with 35 individuals who did not). In agreement with the usefulness of model terms were 184 companies; while 31 companies did not find this approach useful. Thus, among companies and individuals about 83% would find guidelines and checklists useful.

The question asked of respondents was, "From your perspective, would it be useful if model Service Level Agreements (SLA) or End User Agreements (EUA) existed for cloud services so that certain basic terms and conditions could easily be incorporated into the contractual agreements?".

The need of having model contracts for SLAs and EUAs at European level is a widely shared opinion among all respondent groups. Typical statements from respondents are:

> "*A model SLA or EUA will help Cloud services to define the rights and responsibilities of all involved parties."* Another statement*: In addition, it would be useful if an EU 'certified' service, meeting clear defined EU criteria, would exist";*
>
> *"Standard ratified models, agreements or "sections of" should be available covering the different aspects of delivery and for different purposes/levels of cover. It can then be up to the user and provider to agree which they want/need to apply to the particular service they are procuring/providing".*

Respondents to this question touched upon other issues: It is important that the clauses are **simple**, **clear** and should be **accepted** by all involved players:

> "*As a European cloud provider, our experience in contracting cloud computing services, as a provider as well as a customer, has shown that it is useful to include standard clauses of terms and conditions, provided these clauses are clear and simple in their wording as well as in their meaning.*

The issue of different legislation in different Member States was also raised:

> "*Since legislation varies across the member states, it would definitely be very useful to have some templates that would apply to all states. Improvement of SLA's and EUA's must obviously be parallel with improved consistency of judicial and regulatory approach…."*

The advantages of this approach for SMEs were mentioned. Typical opinion is expressed by the following quote:

> *"European SMEs that buy or sell services from other nations within the EU would benefit greatly from having model Service Level Agreements or End User Agreements for Cloud services. Such an agreement would provide some legal certainty for SMEs who, due to their nature, often lack resources to develop or review agreements necessary for cross-border Cloud transactions."*

Opinions were divided on whether updates to **the EU Data Protection Directive** (DP) would facilitate cloud computing while preserving privacy, although more answers were positive than negative both for individuals and companies. Here, of the 152 individuals who answered the question, 86 answered, "Yes", while 66 said, "No". Companies showed a similar division: on the affirmative side were 114 companies and on the negative were 89. Many respondents raised issues connected to data protection while responding to other questions, such as liability or determination of jurisdiction.

> *"There are updates to the current Data Protection Directive that which could facilitate the adoption of cloud computing. As we highlighted in our response to the public*

consultation [on data protection] in January 2011, we believe that the DPD revision provides an important opportunity to reduce the complexity and costs associated with the current rules governing the international transfer of personal data inside and outside the European Union. Cloud service providers are increasingly organized on a global scale and apply security standards that are independent of the geographical location of data processing."

The cloud provider industry has often reported that the **diversity of Member State transpositions** of the DP directive have created barriers to cloud computing developing beyond Member State borders. However, respondents to this consultation were divided and gave a large number of "don't know" answers. While 115 individuals and companies indicated that Member State specificities caused difficulties, 139 indicated that they did not. Public administrations tended to be equally divided on whether there is a barrier due to Member State specificities (14 from 31 respondents). Overall, a total of 156 respondents from 489 on this question replied Don't Know. Among the reasons expressed for answering "yes" to this question were the following, some of which illustrate the respondent's uncertainty and confusion:

"Compliance difficulties are magnified due to the fact that there can be wide differences between implementation of the Directive in the 27 EU member states, so solutions that work in one country may not work elsewhere.";

"We have gathered information from 13 EU countries,… namely: Belgium, Czech Republic, Finland, France, Germany, Hungary, Italy, Netherlands, Poland, Slovakia, Spain, Sweden and the UK. For most of those countries, we are not aware of any data protection rules or legislation preventing the use/provision of cloud computing services. However, the following observations must be made: • Under Czech law, the service provider would most likely be considered a data processor but that would depend largely on the nature of services; • Under Finnish and Swedish law, especially concerning public entities, there may be provisions regarding security restrictions which could prevent the provision/use of cloud services; • In France, controllers need to specify the exact third countries to which data are to be transferred in order to obtain an authorisation from the French Data Protection Authority. Note that a report from the National Assembly dated 22 June 2011 ("Rapport d'information sur les droits de l'individu dans la révolution numérique") suggests drafting new legislation, where cloud computing solutions located outside the EU would be barred from processing sensitive data. Presently, there is no indication that this proposal will be turned into law; • Under German law, cloud providers are seen as data processors. Both the strict, impracticable German requirements for data processing agreements and the particular view of German data protection authorities on Safe Harbor are major issues for cloud computing. There are even opinions of German data protection authorities that cloud computing, in particular in non-EU/EEA-clouds are not legally possible at all; • The Italian Data Protection Authority issued a general Resolution - published in the Official Gazette No. 153 of 4 July 2011 - outlining a new principle for the appointment of data processors by companies which outsource personal data to external agencies…";

"…the requirement that always the local data protection laws applicable to the controller shall apply to the respective processing relationship is a challenge";

"…it is important to note that cloud computing providers do not always adapt their services to the specific rules of each country of the EU, where their services are provided. This is demonstrated by the fact that the terms of service are the same for all

countries, while the uncertainty as to the question of jurisdiction and applicable law is used by cloud providers as an "excuse" in order not to comply with the specific provisions of each Member State";

"SMEs face several barriers when deploying Cloud-based solutions. The lack of harmonisation within Data Protection rules across the EU is one of the most important. The extent of regulation in Europe and the variations of the rules in different EU member states have created some confusion and misperceptions, often leading to exaggeration of the scope and intentions of such rules. SMEs do not usually have legal staff to assess such ambiguities about the scope of the law. They need not only regulatory clarity and transparency, which would be improved by further harmonisation of the Digital Single Market, but also wider understanding among potential customers of what can be done under existing data protection laws.";

"The revised [Data protection] Directive has to ensure a secure and efficient flow of data across national and international borders and must harmonise the data protection rules in the 27 Member States in order to facilitate companies operating across borders. The lack of uniformity in data protection rules creates enormous challenges for entrepreneurs….";

"[A Dutch SME] has been informed by Luxembourg's authorities that animals' rights to data privacy would inhibit the company's ability to market its product widely in the 27 Member States and that Luxembourgers' data must be stored in servers located within the country.";

"Bei vielen Cloud-Services herrscht eine große Unsicherheit über die Rechte der Anwender und die Pflichten der Anbieter. Häufig sind die Parteienkonstellationen kompliziert. Beispielsweise spielt nicht nur das Verhältnis Cloud-Nutzer zu Cloud-Anbieter eine Rolle, sondern vielmehr Verbraucher / Betroffener zu einem Cloud-Nutzer, der wiederum im Verhältnis zu einem zu Cloud-Anbieter steht…. Weitere Unklarheiten besonders hinsichtlich des Datenschutzes entstehen dann, wenn die Daten in verschiedenen Rechtsräumen, insbesondere außerhalb der EU, verarbeitet werden. Fragen nach der Durchsetzbarkeit der Rechte der Verbraucher sind dabei oft ebenso ungeklärt wie die – zum Teil sogar vertraglich verpflichtende - Möglichkeit des Zugangs Dritter (zum Beispiel staatlicher Stellen beziehungsweise Sicherheitsdienste) zu den in der Cloud gespeicherten Daten. Weiterhin ist oft nicht klar, ob / wie die Daten durch den Cloud-Anbieter noch genutzt warden…. Daher müssen dringend Anforderungen geschaffen werden, um für die notwendige bessere Transparenz der Rechte und Pflichten von Benutzern und Anbietern zu sorgen. Dabei muss auch geklärt werden, wie diese Rechte praktisch durchgesetzt werden können[2]"

---

[2] In many cloud services there is a large uncertainty about the rights of users and the obligations of providers. Often the constellations of the concerned parties are complicated. For example, it is not only the relationship between cloud users and cloud providers which matters, but to a high degree the relationship between consumers / users affected to a cloud user which in turn has a relationship to a cloud provider .... Further confusion especially with regard to data protection arise when the data are processed in different jurisdictions, particularly outside the EU. Questions about the enforceability of the rights of consumers are often equally unclear how the - sometimes even contractually binding - possibility of access by third parties (for example, state agencies and security services) to the data stored in the cloud. Furthermore, it is often not clear whether / how the data will be used by the cloud providers .... Therefore it is urgent to determine requirements to provide the necessary increased transparency of the rights and obligations of users and providers. It must be also clarified how these rights can be enforced in practice.

Since the public sector can play a role in stimulating the use and take-up of cloud computing, respondents were asked to list **Member State initiatives** of which they are aware in the area of Cloud Computing. They were asked to comment on whether these initiatives are adequate, go too far or not far enough to help stimulate the market. Respondents were left to explain their views. Of 145 responses 94 (64%) indicated that Member State initiatives do not go far enough.

> *"The public sector must lead by example. By being early adopters of cloud technologies – including via pre-commercial procurement – public authorities can educate the private sector about the benefits of the cloud and encourage private sector uptake. In this regard, as in all areas of procurement, [this organisation] encourages public authorities to be technology neutral and to choose the best technology or service for the particular need…";*
>
> *"Pan-European infrastructures such as Géant for networking and EGI for computing have allowed different resource providers to collaborate directly. This collaboration has significantly improved communication between the various providers and created a framework in which appropriate standards and best practices can emerge. The public sector should look to existing infrastructures (where possible) as a mechanism to continue the push towards practical standards and best practices.";*
>
> *"No – private industry cloud procurements should enable business activities not directly supporting competitive advantage, while public sector cloud procurements are not concerned with maintaining competitive advantage (of the public sector). Furthermore, private industry's other commercial concerns such as achieving Return on Investment targets, are not also held by public sector entities. The EU public sector can act as an example by procuring those cloud services which offer cloud products best suited for the EU market; and by encouraging specific types of cloud vendors and providers.";*
>
> *"Yes. The public sector has the opportunity to play an important leadership role through the deployment of eGovernment and eScience infrastructures. The most effective way for the public sector to shape the evolution of the Cloud is not through law and regulation but by being smart users of the technology."*

The need for **future research** to improve current cloud computing commercial offerings was broadly agreed. Of the 312 respondents to this question, 241 (77%) confirmed the need for additional research, compared to 71 who found it unnecessary. Of a total of 381 respondents, 222 (58%) considered that public funding was appropriate for this sort of research.

The question asked was, "…. do you see technical problems/limitations of current cloud service offerings that will require further research in the coming years?" Typical of opinions expressed in response are the following quotations.

> *"Management of hybrid deployments**….** involves a number of complex issues. It requires the ability to manage multiple interdependent virtual machines and data resources, geographically distributed…. Support for time critical or real-time and interactive applications will also require additional research." …."communication networks, including wide-area (Internet, NGN, wireless). Support for time critical or real-time and interactive applications will also require additional research.";*

"Development of the Internet of Things (IoT) and Machine-to-Machine (M2M) communications are two of the fastest growing segments of SSBS. Support of these applications will impact cloud service offerings due to the expected huge numbers of active entities…"

The consultation recognised that Cloud Computing is a global infrastructure. Respondents were asked, "What are the most important Cloud Computing problems that have to be discussed at a global level?" Respondents were also invited to identify the most appropriate fora in which discussion might take place. Respondents emphasised the **global nature of computing** and the expectations of users to be able to access their data and services from anywhere at any time. Answers were given in free text. Typical of the problems to be solved in international fora were:

"the legitimate need of global businesses, for both commercial and compliance purposes, to maintain a single global picture of their operations across multiple jurisdictions and therefore to maintain global databases, which require widespread sharing of personal data and other information between the members of corporate groups"

And further:

"Legal aspects: data privacy and protection, jurisdictions, rights and responsibilities; they are cross-cutting issues and need the involvement of the European Commission. • Technical aspects: standards and best practices.";

"International data transfer compliance mechanisms do not provide effective data protection for customers or legal certainty for companies. More broadly, we encourage the Commission to discuss these issues with international groups like the G8/20. "

Conclusion

The EU **legal framework** within which Cloud Computing must be implemented confuses and creates uncertainty in the respondents to the consultation. There is a widespread need for clarification on rights, responsibilities, data protection and liability, especially in cross-border situations. Guidelines on good practice in contracting, model terms and conditions, reasonable expectations for service level agreements would be appreciated. The **public sector**, as cloud computing adopters, could set the requirements for standards in security, interoperability and data portability; thus, stimulating rapid deployment. Resolution of the single digital market issues is only a partial solution since Cloud Computing is inherently embedded in a global infrastructure. It follows that **international agreements** on certain principles such as certification, data protection and security are needed. Finally, current Cloud Computing is capable of improvement through **research and development**, notably integration of other distributed computing models.