

**Project Number: 034702**  
**Project Acronym: BEinGRID**  
**Project Title: Business Experiments in Grid**  
**Instrument: Integrated Project**  
**Thematic Priority: Advanced Grid Technologies, Systems and Services**

## D2.6.9 – Final set of legal guidelines for Grid business

*Activity 2: Business Common Cross-Activities*

*WP 2.6: Legal Issues*

<b>Due Date:</b>	M39	
<b>Submission Date:</b>	15/10/2009	
<b>Start Date of Project:</b>	01/06/2006	
<b>Duration of Project:</b>	42 months	
<b>Organisation Responsible for the Deliverable:</b>	K.U.LEUVEN - ICRI	
<b>Version:</b>	1.2	
<b>Status</b>	Final for submission	
<b>Author(s):</b>	Davide M. Parrilli	K.U.LEUVEN - ICRI
<b>Reviewer(s)</b>	Mark Sawyer	EPCC
	Helene Huard	CRSA

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)

**Dissemination Level**

<b>PU</b>	Public	<b>X</b>
<b>PP</b>	Restricted to other programme participants (including the Commission)	
<b>RE</b>	Restricted to a group specified by the consortium (including the Commission)	
<b>CO</b>	Confidential, only for members of the consortium (including the Commission)	

---

## Version History

<b>Version</b>	<b>Date</b>	<b>Comments, Changes, Status</b>	<b>Authors, contributors, reviewers</b>
1.0	30/09/2009	First version for internal review	Davide M. Parrilli (KULEUVEN – ICRI)
1.1	14/10/2009	Final version after internal review	Davide M. Parrilli (KULEUVEN – ICRI)
1.2	15/10/2009	Final format check	Julia Wells (ATOS) Karita Luokkanen-Rabetino (ATOS)

## Table of Contents

<b>1. EXECUTIVE SUMMARY</b>	<b>5</b>
<b>2. INTRODUCTION AND PURPOSES</b>	<b>6</b>
2.1 REFERENCES	8
2.2 GLOSSARY OF ACRONYMS	9
<b>3. LEGAL REQUIREMENTS, GUIDELINES AND TIPS FOR TECHNOLOGY PROVIDERS, SERVICE PROVIDERS AND USERS</b>	<b>10</b>
3.1 SERVICE LEVEL AGREEMENTS	11
3.1.1 <i>Tips for technology/service providers</i>	11
3.1.2 <i>Tips for end users</i>	11
3.2 TAXATION	12
3.2.1 <i>Tips for technology/service providers</i>	12
3.2.2 <i>Tips for end users</i>	16
3.3 INTELLECTUAL PROPERTY RIGHTS	17
3.3.1 <i>What about going open source? Licensing strategies</i>	17
3.3.2 <i>Copyright issues: liabilities and third parties</i>	18
3.3.3 <i>Patentability issues and risks of infringing existing patents</i>	19
3.4 DATA PROTECTION AND SECURITY	20
3.4.1 <i>Data protection in Grid and Cloud computing scenarios: what to do?</i>	20
3.4.2 <i>Security issues: legal approach and tips</i>	22
3.5 THE COMPLEXITY OF THE GRID AND CLOUD BUSINESS FROM THE LEGAL POINT OF VIEW	23
<b>4. CONCLUSIONS: CHECK LISTS FOR TECHNOLOGY PROVIDERS AND SERVICE PROVIDERS</b>	<b>26</b>
4.1 LEGAL ISSUES ARE NOT ENOUGH: CHECK LIST FOR TECHNOLOGY PROVIDERS	26
4.2 SERVICE PROVIDERS: TO WHAT EXTENT ARE THEY DEPENDENT ON TECHNOLOGY PROVIDERS?	27
<b>ANNEX A. LICENSE CONDITIONS.</b>	<b>29</b>

## 1. Executive summary

Technology and service providers must pay attention to several legal issues that are likely to affect their business. In particular, in the course of the project, we found out some specific areas, namely:

- **Service Level Agreements:** the market of commercial Grids and Clouds is dominated by a few big international players that usually impose provisions that do not protect adequately the interests of the clients. Therefore, service providers that supply services using the infrastructure of technology providers should negotiate as much as possible the content of the SLA they enter into and should also contract a plurality of providers, as to minimise the risks linked to security failures.
- **Taxation:** tax aspects are absolutely important and affect primarily technology providers, mainly in the area of income taxation. The tip that we can give to technology providers that want to set up a transnational Grid or Cloud is to select countries that do not consider Grid and Cloud components being permanent establishments of the company, as to reduce the overall tax burden. This strategy, called 'tax planning', may regard also indirect taxation, at least at European level, where VAT applies.
- **Intellectual Property Rights:** in the field of copyright, licensing strategies should be taken into due account, and technology and service providers could think about providing open source solutions (this issue is relevant especially for service providers). It is advisable to opt for a standardised open source available in the market or to adapt an existing one to the specific needs of the business case. Copyright regards also liabilities towards third parties, and with this regard the companies involved shall avoid to infringe existing third parties rights. The same applies to patentability issues, given the fact that a certain software may be unpatentable in Europe but being protected by a patent in the United States.
- **Data protection and security:** in the former field, privacy regulations must be taken into due account and the best strategy to avoid or reduce risks is not to collect personal data. In some cases, like in e-health Grids, this is simply impossible, but the actors involved (service and technology provider) shall state clearly who is liable for what. They shall also verify which authorisations are necessary and they should set a user-friendly privacy policy.

Other legal considerations will be developed as well, together with some final remarks about Grid and Cloud computing from the lawyer's perspective.

## 2. Introduction and Purposes

This Deliverable is the last document produced by BEinGRID in the framework of WP2.6 devoted to legal issues. It represents the last step of a long journey where we approached a new and fascinating topic, Grid computing, we got familiar with it and tried to show its critical points and all its potential from the legal perspective.

Forty-two months are a long period of time. Many things changed in these years, starting from the notion and the characteristics of Grid computing. Grid computing is going to be replaced, at least formally, by Cloud computing. Cloud computing is more actual than Grid computing, and this has an impact also on our work and our WP. The first question to answer is very radical: is the work performed so far still actual and useful? Potentially, there is the risk that the work performed so far in the field of Grid computing is useless and definitely outdated.

The answer to this question is a very strong 'no'. The work performed is not outdated but is more actual than ever. In these forty-two months we made research, we produced deliverables, we published articles and book chapters, and we attended conferences: in other words, we were following the evolution of Grid computing and we realised, together with all other partners of BEinGRID, that the paradigm of Grid computing was changing. Therefore, our approach was not static but extremely flexible and dynamic. We wrote about Grid computing, but we were referring to Grid computing and to all other, existing and future, similar technologies. We had, and we still have, in mind the notion of dispersed resources. Grid computing has been pioneering in this sense: the use of dispersed computing and storage resources is pivotal in understanding the future of ICT. This goes beyond the traditional, static notion of outsourcing, and this element characterises also Cloud computing.

After many deliverables and publications, we can say that our work has been pioneering in the sense that we addressed the legal issues linked to the adoption of dispersed resources by ICT companies and users. The technological panorama changed and lawyers cannot just neglect that or, even worse, state that all old principles must be adopted uncritically or that the use of dispersed resources is not compliant with existing laws and regulations.

The message that we gave, and we still give, is positive: the Law is not a barrier to the adoption of Grid and Cloud technologies. Legal issues must be taken into due consideration, but at the end we believe that static and illogical legal principles cannot limit the development of efficient and useful technologies. We reject the idea 'it's too cumbersome to be done': if the business plan is good, no laws can say that dynamic and intelligent business people must stop and follow traditional paths.

This is clear in the field of privacy and taxation, just to name two examples. Outsourcing of ICT functions with transfer of personal data is not easy to accomplish without breaching existing laws and regulations. However, very often, problems can be avoided with a careful privacy policy and without neglecting to obtain the necessary authorisations by the privacy authorities concerned.

In the field of taxation, difficult issues may arise as well, but at the same time the implementation of intelligent tax planning strategies may potentially avoid or limit problems. Of course, often it would be necessary that public authorities, at national, European and international level, change existing guidelines and regulations and, first of all, modify their approach and mentality. We saw, for instance, that the extension of the notion of permanent establishment to servers and Grid/Cloud components may potentially prevent the development of these technologies: in our view, treating a datacentre that, in a Grid/Cloud computing scenario, collaborates with other resources located in other domains or countries, in the same way as a factory that produces cars, is simply a non-sense from the legal and

business point of view. We understand that international and national authorities are afraid that ICT companies can make huge profits without paying any tax, but taxing these profits in the place where Grid/Cloud resources are located is certainly not efficient and, at the end, not useful for both companies and governments.

At the same time, however, we have to admit that it is not reasonable to be absolutely optimistic about the future massive adoption of Grid and Cloud technologies by companies and individual users. We are not so sure, in the light of the experience gained in these years, that businesses and consumers are ready to outsource the storage or processing of their files to external Grid/Cloud providers. There are many risks associated to this: losing control over his own files and data is risky. Users have to change their cultural attitude and, above all, it is necessary that they trust providers. From the legal point of view, we can say that the time of trust has not come yet. This depends probably on the same Grid/Cloud providers: we analysed recently the Service Level Agreements (SLAs) frequently adopted (and imposed, at least as regards the content of the SLA) by big international technology providers, and we realised that they tend to limit their liabilities as much as possible. A rational user 'required' to agree on this SLA is likely to believe that providers limit their liabilities so much because the technology that they adopt is unstable and there are huge risks that data get lost or corrupted. We cannot actually blame the users for that!

In other words, security is the big risk in Grid/Cloud computing environments. We cannot, of course, say how to solve it, but we can show how the risk can be mitigated and balanced through contracts. It is not fair that the customer faces the entire risks linked to deletion of data, and it is not right that the providers promise the respect of a certain Quality of Service (QoS) level but that no mechanisms (compensation, damages, etc) exist if this level is not met in practice. The mere adoption of service credits is surely not enough to protect the customers and make sure that their rights are restored when necessary.

It is true, then, that when providers sell Grid/Cloud services to consumers stringent regulations apply and many clauses included in the SLAs are simply null and void, at least according to the applicable European legal framework. But in practice this cannot be enough, and surely it is not useful to build trust towards technology and service providers. We do not believe that consumers are expected to store important files in the Grid/Cloud if the provider imposes clauses that are null and void. Probably many consumers do not realise that many articles in the SLAs they sign are null, but at the same time it is true that there are no clear indicators of the fact that individual customers widely use Grid/Cloud services.

In the next pages we will provide technology/service providers and users with tips about how to run successful Grid/Cloud businesses and how to protect their rights and interests. Therefore this Deliverable contains a set of requirements and guidelines in a form that is easy to understand and concise. The readers, in fact, can find more details in all previous Deliverables and in the publications made in the framework of BEinGRID. This document is also intended to be published in Gridipedia, so that it can reach a wide audience and be downloaded as a flexible booklet where a certain amount of useful information is contained.

Of course these pages are not exhaustive, in the sense that we cannot take into consideration all existing national and regional laws and regulations. This paper is based on legal principles currently accepted and on the European framework, duly analysed in great detail in all previous Deliverables. Awareness is surely one of the keys for the success of Grid/Cloud technologies. The actors involved shall be aware of what they can and cannot do, of what is legal and is not, of what is convenient and what is detrimental. The experience of the writer shows that many Grid/Cloud researchers devote huge efforts to develop systems and applications for e-negotiations of contracts, like SLAs, but these agreements that are created with no human intervention and control may be declared null and void by a judge

who has to solve disputes linked to the implementation of the contract. Lack of awareness means that time and money is devoted to have an application that in practice is not likely to be used by any business because, legally speaking, is too risky and vague.

We hope that we can help, at least in a very small scale, to increase the knowledge of legal issues within the technical and business audience. The mixing of different sciences, mentalities and approaches is, ultimately, absolutely necessary to develop technologies that are usable and useful.

## 2.1 References

Please refer to all references of D.2.6.1, D.2.6.2, D.2.6.3, D.2.6.4, Activity 2 Meta-deliverable, D.2.6.6, D.2.6.7 and D.2.6.8.

Furthermore, the following publications made in the framework of BEinGRID project are relevant:

Stanoevska-Slabeva, K., Wozniak, T., Thanos, G., Parrilli, Davide, Serrabou, B., Luokkanen-Rabetino, K. (2009) Turning Grid Research into Business - Identification of Commercialization Barriers. In: Proceedings of the First International ICST Conference on Digital Business (DigiBiz 2009): Springer, 2009 - The First International ICST Conference on Digital Business (DigiBiz 2009). - London, UK, S. 8. - ISBN 978-963-9799-56-1;

Parrilli, Davide M. (2009) Grid and Cloud Computing as a Tool to Transform European Economy: Legal Considerations, paper presented at the Conference FITCE 2009, Prague, 5 September 2009;

Parrilli, Davide M. (2009) The Determination of Jurisdiction in Grid and Cloud Service Level Agreements, in Altmann, J. et al. (Eds.), Grid Economics and Business Models, Lecture Notes in Computer Science, no. 5745, Springer, Heidelberg, pp. 128-139;

Parrilli, Davide M. (2008) E-Commerce and Transfer Pricing. Some Selected Issues, in Masaryk University Journal of Law and Technology, vol. 2, no. 2, ISSN 1802-5943, pp. 83-97;

Stanoevska, K., Parrilli, Davide M. & Thanos, G. (2008) Defining Efficient Business Models for Grid-enabled Applications, in Cunningham, P. & Cunningham, M. (Eds.), Collaboration and the Knowledge Economy: Issues, Applications, Case Studies, ISSN 1574-1230, IOS Press, Amsterdam, pp. 1113-1120;

Parrilli, Davide M., Stanoevska, K. & Thanos, G. (2008) Software as a Service (SaaS) Through a Grid Network: Business and Legal Implications and Challenges, in Cunningham, P. & Cunningham, M. (Eds.), Collaboration and the Knowledge Economy: Issues, Applications, Case Studies, ISSN 1574-1230, IOS Press, Amsterdam, pp. 633-640;

Stanoevska-Slabeva, K., Parrilli, Davide M. & Thanos, G. (2008) BEinGRID: Development of Business Models for the Grid Industry, in Altmann, J. et al. (Eds.), Grid Economics and Business Models, Lecture Notes in Computer Science, no. 5206, Springer, Heidelberg, pp. 140-151;

Parrilli, Davide M. (2008) The Server as Permanent Establishment in International Grids, in Altmann, J. et al. (Eds.), Grid Economics and Business Models, Lecture Notes in Computer Science, no. 5206, Springer, Heidelberg, pp. 89-102.

## 2.2 Glossary of Acronyms

Acronym	Definition
B2B	Business to Business
B2C	Business to Consumer
BE	Business Experiment
BEinGRID	Business Experiments in Grid
CPU	Central Processing Unit
D	Deliverable
ECJ	European Court of Justice
EU	European Union
ICT	Information Communication Technology
IPR	Intellectual Property Right
OECD	Organisation for Economic Cooperation and Development
QoS	Quality of Services
RaaS	Resource as a Service
SaaS	Software as a Service
SLA	Service Level Agreement
UK	United Kingdom
US	United States
VAT	Value Added Tax
WP	Work Package

### 3. Legal requirements, guidelines and tips for technology providers, service providers and users

Grid and Cloud computing are basically based on the paradigm of outsourcing. In the field of ICT outsourcing is not new, and therefore the experience gained in the legal domain until now is applicable. But Grid and Cloud computing amplify the issues and problems of outsourcing due to the use of dispersed resources and to the fact that, potentially, both hardware and software resources can be hosted remotely. Furthermore, many parties are involved in a Grid or Cloud value chain, especially if we consider the typical SaaS value chain. Many places, and thus potentially many applicable laws, are also involved: the place where the SaaS provider is located, where the technology provider is established, where the Grid/Cloud components (datacentres) are located, where the end user is domiciled, where the end user uses the services, etc.

The problems linked to the 'volatility' of the Internet, to the outsourcing in the ICT sector, to the adoption of dispersed resources, to the virtualisation and dematerialisation of goods and services are combined and made bigger by Grid and Cloud technologies. But this does not mean that these novelties must be rejected: to the contrary, new problems require new solutions, and lawmakers/public authorities must accept the challenges and the responsibilities that are required to them. One perfect example is the notion of consumer: all existing legal sources at European level state that consumer is only the physical person acting outside his trade or profession. Therefore, all business entities, even micro-enterprises, are not deemed to be consumers. This is clearly stated in the laws and the courts called to interpret them who, starting from the ECJ, rejected all different interpretations. The question is: is it fair that professionals and micro-businesses are excluded from the notion of consumer? To give a concrete example: when a company with one employee and a yearly turnover of half million euro buys Cloud capacity from Amazon, can we say that the parties are in equal position, just because they are both businesses?

No protection is basically granted to this micro-enterprise: Amazon can state that it is never liable if the customer's data get lost or corrupted, that American law is applicable to the contract and that all disputes shall be solved by an American court. Can we really imagine that the customer will try to enforce his rights if they are breached by Amazon? Provided that we can talk about rights of the customer, as they are very limited!

Maybe the European Commission should start thinking about extending the notion of consumer, or to alter completely the level of protection for customers in general. This raises also political and philosophical problems: do we want a lawmaker that regulates everything and acts like a good father or instead a lawmaker that watches what happens in the society and intervenes only if and when necessary? Personally, the author prefers the latter model, and in theory it is better that parties are free to regulate their interests in the market. In this sense, Amazon can impose what it wants, customers can accept it or not, but if there is no fraud involved they cannot complain for the lack of protection granted by the contract they signed. Ultimately, of course, we can expect that many small businesses will never use Grid or Cloud services due to the risks involved. And obviously it is not very rational to give all data and files to an external technology provider knowing that if something goes wrong no compensation will be due, apart from some risible service credits.

We will now focus on some specific issues, and we will show what technology/service providers and clients should and should not do.

## **3.1 Service Level Agreements**

### **3.1.1 Tips for technology/service providers**

We take into consideration two different scenarios: (i) provision of Grid/Cloud storage and computing capacity to an end user; (ii) supply of Grid/Cloud-based services (e.g. SaaS) to an end user using the Grid/Cloud infrastructure of a provider, third party. In the former case there is only one SLA, between the technology provider and the end user. In the latter situation, there are two SLAs, one between the technology provider and the service provider and the other between the service provider and the end user.

The interests of technology and service providers may differ, as well as the size of the two businesses. Usually, in fact, Grid/Cloud providers, with the exception of academic institutions, are big companies while, on the other side, service providers may be small undertakings that, in fact, develop and commercialise software without managing any datacentre. The SLA between the two parties shall be tailored to the needs of the specific business relation and therefore there are grounds for negotiations. We doubt, in fact, that standard SLAs are, in most cases, fit to be used when the technology provider must host software or other applications of a service provider to be delivered to end users.

The most relevant tip for the technology providers is to be fair, i.e. not to impose clauses which deprive customers of all their rights. Technically speaking, SLAs should not contain clauses that are null and void. This is the case in point with articles proposed/imposed to consumers when the position of the provider is too unbalanced in comparison with that of the consumer. In other words, generally speaking, according to the applicable European legal framework a contract can not foresee that the provider has only rights and the client/consumer only obligations. Very often SLAs reach this result in a more subtle way, i.e. imposing obligations also to the provider (logically, the provision of the service, the respect of a certain QoS, etc) but stating that the lack to respect these obligations is without any sanction.

Clauses that are typically null and void, or voidable according to the applicable national legal framework, are those that confer to one party, usually the provider, the power to unilaterally modify the contractual conditions, those that exclude the liability of the supplier, those that confer exclusive jurisdictional competence to the court of the place where the provider is domiciled, etc. In some countries, e.g. in Belgium, the adoption of illicit clauses with a plurality of consumers can bring to an administrative complaint filled by the consumers' associations and to a fine.

This risk does not exist in the SLA between the technology and the service provider since the latter is a business and no protection for consumers applies. In this case the service provider should try to negotiate with the technology provider and balance his rights with the ones of the counterpart in the SLA. In principle, in fact, the service provider is not protected by the applicable legal framework like consumers are. In some circumstances, the technology provider cannot limit or reduce his liability but this happens usually for damages arising from hardware components (e.g. a computer originates a fire that damages the premises of the service provider). But in the relationship between a Grid/Cloud supplier and a service provider there is no transfer of hardware involved (the delivery of the hosting and computing service is outsourced), thus the above rules, if any, do not apply.

### **3.1.2 Tips for end users**

End users buy storage or computing capacity from a Grid/Cloud provider or software, resources, applications, etc from a service provider. They can be consumers or businesses, and tips shall be given taking into account these difference. European consumers, in fact, are to a certain extent protected by the applicable laws, so that many clauses in the SLA are

deemed to be null and void. The tip that we can give to them is to carefully control the contract they enter into and to verify whether or not there are illicit provisions. According to the country where the dispute arises, or whose laws are applicable, illicit clauses can be void or voidable. In the former case, basically, the judge in charge of the dispute will declare the nullity of the provisions even if the party concerned did not ask that; if the clauses are voidable, the declaration can be pronounced by the judge only after due request by the consumer. In any case, it is advisable that the consumer writes in his summons which clauses of the SLA are void or voidable to be sure that the judge will make an investigation.

When the consumer can claim that some provisions of the SLA are illicit? Rules differ from country to country, but basically the consumer can decide to sue the provider even if no other disputes have arisen (e.g. regarding the respect of the promised QoS, the price, etc) or to claim the nullity of the clauses in connection with another claim. Typically, it can happen that the consumer suffered damages arising from the incorrect delivery of the services and he sues the provider to obtain compensation. At the same time, the consumer asserts that some clauses are void and inapplicable (e.g. those regarding the limitation of liability of the provider).

Very often suppliers know that inserting void or voidable provisions in the SLAs entered into with their clients is not particularly risky. Insofar as no other issues will arise, the customers are not likely to sue them. Honestly, if no other serious issues are involved, it is not very advisable for a consumer to sue a provider, since he has to bear some costs and, economically speaking, this is not efficient, even if these costs are then refunded by the provider once he is convicted.

Things are different in those countries where the associations representing the consumers' interests can sue the companies that make use of illicit clauses. In this case it is efficient for a consumer to complain about the behaviour of the supplier with the association and the association, if the complaints are many, will probably sue the company. The judge then will convict the provider to use more correct provisions. Problems, in practice, do arise if the technology or service provider is domiciled in another country or continent. Just to make an example, many provisions in the SLAs proposed/imposed by big commercial Grid/Cloud providers are void according to the applicable European legal framework but these providers are established in the United States.

In this case, the association of consumers' in the European States cannot do a lot against these practices, and, in practice, the clients can only decide not to buy services from these suppliers or to opt for suppliers, if any, domiciled in Europe or in their country of residence.

## **3.2 Taxation**

### **3.2.1 Tips for technology/service providers**

Taxation is one of the fields where Grid and Cloud computing shows very clearly that the use of dispersed resources introduces new problems and issues and that, unfortunately, the law and policymakers are not aware of this. The research performed within BEinGRID focused on direct and indirect taxation, i.e. respectively on (i) taxation of profits and incomes generated by the technology/service provider and on (ii) taxation of the Grid/Cloud services supplied to end users. The analysis of direct (income, corporate) taxation has been based on the international legal sources applicable and furthermore we performed a comparative analysis among several jurisdiction, in Europe and outside Europe. As regards indirect taxation, the research has been essentially focused on the legal situation in the EU, since in Europe there is a set of rules (in the field of VAT) devoted to electronically supplied services.

In the field of international direct taxation, the concept of permanent establishment and its applicability in the ICT sector are of pivotal importance. The OECD devoted great attention to

the concept of server as permanent establishment, and states that if a company has a server in another country, and if some criteria are met, the server is deemed to be a permanent establishment of the company and therefore taxes are due in the country where the server is located for the profits generated there. The OECD cannot enact binding laws, and therefore what we said is a principle widely accepted by the most developed economies in the world, but exceptions do exist.

Saying that a server is a permanent establishment, i.e. the presence of a server is a reasonable ground for taxation of profits, is viable in simple e-tailing scenarios. If a company located for instance in France has only one server in Belgium and this server carries on all the business functions of the enterprise, it is reasonable that profits are primarily taxed in Belgium. But this is not the case in point as regards Grid and Cloud computing. These technologies do not rely on the use of only one server that concentrates all business functions, but rather on dispersed resources that can be located in several jurisdictions.

One point must be clear: the fact that a company with datacentres located in several countries must pay taxes in all those countries is not correct from the theoretical point of view and not feasible in practice. We omit here all theoretical considerations, and we rather focus on practical issues. The use of Grid and Cloud technologies renders cumbersome the determination of the portion of profits generated by every Grid/Cloud component, i.e. by every datacentre. Since these components are deemed to work together and to create a unique environment, although geographically dispersed, it is not easy, and probably not possible neither, to assess which business function is attributable to a specific component.

However, this fact has not been accepted yet by many countries. To be precise, there are no precise guidelines about tax treatment of Grid and Cloud components, but taxation of servers and datacentres is not a new issue. It is likely that tax authorities simply apply the regulations applicable to servers that carry out all business functions of a company to Grid and Cloud datacentres, even if, from the technological and commercial point of view, the two scenarios are dramatically different.

The main suggestion for technology and service providers is to implement a careful tax planning strategy. It has to be said that only technology providers are affected by the tax issues linked to the location of Grid and Cloud components, as service providers are supposed not to own and manage their own datacentres. However, tax planning regards both providers, and it has to be focused on the location of the principal place of business of the company and, if it is the case in point, on the location of the Grid/Cloud infrastructure.

The first step in tax planning for Grid/Cloud enterprises is the location of the principal place of business, i.e. of the place where the company is resident. ICT allows great mobility and volatility for businesses, and if the company provides virtual services, no link with a particular country or region is necessary. One point must be clearly highlighted: tax aspects are not the only ones to take into consideration when deciding the place of residence of a company. Many other factors shall be considered as well. In particular, many governments will not like the idea that their technology providers move to some tropical islands where taxation is very low or not existent, and it is possible that they implement some sort of retaliation strategy against these companies. We can imagine that, for instance, these enterprises will not be allowed any more to contract with the public authorities of the ex State of residence, thus losing probably the best clients. In this sense, service providers enjoy from more freedom than technology providers: especially if they are small or medium-sized companies, they will attract less attention by tax and political institutions.

Furthermore, technical considerations must be taken into account as well. For a technology or service provider the level of connectivity and the quality of the overall infrastructures of the country/region where the company is resident may be very important. A tropical island in the

Caribbean may be a perfect location from the tax point of view, but there are probably better places for datacentres. All tax savings, for instance, may be used to cool down the machines and probably telephone connections are not good enough to serve customers in the United States, in Europe, etc. Yet, things are different for service providers, as their requirements are less stringent than for Grid/Cloud providers.

Another issue for technology providers is proximity with the place where datacentres are located. We assume, for instance, that British Virgin Islands are an excellent location for the principal place of business of a company, i.e. for the place of residence: here the strategic decisions of the enterprise are taken, the managers meet, the company is registered, etc. At the same time, establishing Grid/Cloud datacentres in these islands does not seem to be the cleverest decision. They can, for instance, be located in the State of Washington in the United States. Is it strategically appropriate that the place of management and the datacentres are so far away each other? This must be assessed on a case-by-case basis by the managers of the technology provider. If they believe that there are no particular problems or obstacles, they will act accordingly.

Tax planning should also be realistic: in other words, tax authorities do not like the idea that their nationals manage a company registered in the middle of the Caribbean sea and do not pay taxes in the country where the executives probably live. This concern is highly understandable, but we have to say that there are no grounds to say that locating a company in a tax heaven is *per se* illicit. If the business does not have the function to carry out money laundering activities, it cannot be forbidden to investors and business people to open a company resident in a tax-friendly country.

We have to consider that we live in the era of ICT, where people can communicate without being physically present in the same room. The notion of place of effective management is therefore vague and flexible. We can even say that the place of effective management is likely not to exist any more if the executives of the company make use of technology. The strategic business decisions can be taken via teleconference, many functions can be simply outsourced, etc so that decisions are taken in many places and not centralised in one building or room. Tax planning as regards the place of residence of the company is thus potentially unlimited.

Things are different as regards tax planning applied to Grid/Cloud components. In this field technical considerations are absolutely pivotal and taxation is probably not the most relevant issue when assessing where it is convenient to place a datacentre. To be more precise, taxation is surely important, but other technical and economic factors play a dominant role, e.g. the price of electricity, the cost of labour, climate conditions of the region, etc. However, the location of the datacentres has to cope with the issue of the permanent establishment, as described above. Technology providers should consider which countries do not treat servers and ICT components as permanent establishments (e.g. the UK) since locating there the datacentres can potentially reduce the tax burden and the costs linked to pay taxes in several jurisdictions and to claim refund, if allowed, in the residence country. This analysis may be time-consuming, and it is surely better to ask officially to the tax authority of the country concerned about the tax treatment of the Grid/Cloud components before making the investment. Tax issues are surely a barrier to the implementation of transnational Grids and Clouds, but a careful tax planning may at least reduce these obstacles.

Different remarks can be done in the area of indirect taxation. Given the scope of these pages, we will focus on the European VAT regime applicable to electronically supplied services. The provision of Grid and Cloud computing and storage capacity can be qualified as supply of electronic services ('electronically supplied services' in the language of the applicable European legal sources) and thus a special regime will apply. The same applies to

the provision of SaaS, RaaS, etc. All these services are virtualised, dematerialised, and are delivered in electronic form. Potentially they can be delivered in the form of a tangible asset, but this would go against the paradigm of Grid and Cloud computing. It has to be assessed on a case-by-case basis whether or not a service can be qualified as an electronically supplied service, but in general software, applications, etc downloadable from the Internet and other storage and computing services that are accessed by the user through a web portal are deemed to be electronic services.

As regards practical tips and recommendations, the user cannot do much to avoid VAT. Actually he can, but we would not recommend opening off-shore account just to save VAT. The operation can be risky and its legitimacy can be discussed. Furthermore, businesses can compensate the input VAT with the output VAT. And making fictitious exports outside the EU in order to avoid VAT with the aim to commercialise the good or service inside the EU is a fraud that can justify criminal sanctions. Of course, when we talk about electronic services things are more complicated, and it is impossible to literally talk about export and use inside the EU. Multinational groups may implement VAT tax planning strategies when buying and exchanging services between subsidiaries, but this topic is not really Grid and Cloud-related.

Tax planning may involve the place of establishment of the technology and service provider to offer cheaper services to the customer/consumer. In B2C transactions, in fact, VAT is due, when both provider and client are domiciled in the EU, and the place of taxation is the supplier's country at the VAT rate applicable there. An example will clarify the point. Company A provides electronic services and it is domiciled in Sweden. The price of the services is 100 euro and the applicable VAT rate is 25%. The final price for the consumer will be then 125 euro. Company B provides the same services but it is domiciled in Luxembourg. The price is 100 euro and the applicable rate is 15%. Thus the final price for the consumer will be 115 euro. This shows clearly that for a consumer it is more convenient to buy services from the supplier established in Luxembourg. And this means that for providers it is convenient to be located in Luxembourg in order to be more attractive for European consumers.

This is another aspect of tax planning. The tip we can give to technology and service providers is to take into consideration the tax facilities offered by Luxembourg and think about providing the services from this country for tax purposes. The only disadvantage is that this regime will end in 2015 due to the entry into force of the so-called VAT package 2008. Since 1 January 2015 the applicable rate will be that of the customer's Member State and therefore location in Luxembourg will not be extremely convenient, at least from the VAT point of view. VAT competition between EU Member States will disappear and this is at detrimental of the consumers. In the above examples, the Swedish consumer who buys services from company B for 115 euro will see the price increase to 125 euro due to the application of the Swedish VAT rate. Potentially this can harm the whole market of electronic services. Not all customers will be willing to pay a higher price for the same service, and maybe they will not buy e-services anymore or to a smaller scale.

A further aspect of tax planning regards property taxes. Property taxes are charges imposed by central or local governments to the company's premises and/or to the land where these premises are located. Property taxes affect especially the Grid/Cloud providers since the datacentres need a lot of space and potentially many buildings that host them. Software providers, at least theoretically, do not need spacious premises and even no premises at all. We can imagine in fact a company, providing Grid/Cloud-based services, that is composed of a certain number of employees and partners that work from home, with no office. Furthermore, of course, such a company does not need any database since they adopt the infrastructures provided by a technology provider.

Property taxes may potentially be avoided also by technology providers, but this depends on the technological development of servers and computing machines. Potentially, in fact, Grid/Cloud providers can adopt containers to store their datacentres, thus avoiding, when possible, any property tax since a container is a movable property and not an immovable one. Furthermore, Grid/Cloud providers can decide to locate their datacentres off-shore, like marine oil or gas platforms. Legal and tax consultants have to pay attention to the developments in the field and explore the possibilities to reduce tax burdens thanks to these novelties.

Furthermore, the competent authorities often make tax deals with ICT companies, including Grid/Cloud providers, to attract them or to avoid that they move to other locations where the property tax regime is more convenient for the company. Sometimes, they may amend the applicable legislation to attract investments. A case-by-case analysis is required in order to implement the most useful property tax planning strategy. Of course, property tax planning must be done in combination with other tax planning strategies, especially with the above described direct tax planning. Furthermore, all other non-legal factors must be taken into account: a country may offer to ICT investors no property and corporate taxes, but if the price of electricity is ridiculously high or if the country is missing any adequate telecom infrastructure, the investment in that State will definitely not be worthy.

The analysis of property tax planning gives rise to the possibility to wonder whether more innovative strategies can be implemented. In other words, Grid/Cloud providers may search for the most convenient location for their 'traditional' datacentres, but can they solve the problem with innovative measures? To the ends of these pages, attention should be paid to movable datacentres (i.e. Grid or Cloud components stored in containers) and to the possibility to locate datacentres in the sea (off-shore infrastructure).

Hosting Grid and Cloud components in containers can be interesting also in corporate tax planning. If the container is effectively moved (we would say at least every year), the Grid or Cloud component is not deemed to be a permanent establishment. Of course, moving the containers from one country to another on a regular basis is an extra cost for the technology provider and we doubt that this is the best solution to avoid the permanent establishment problem. However, hosting Grid or Cloud components in containers can be interesting to the ends of property tax, at least in those jurisdictions where containers are exempted from property tax. An example is Oregon (United States), where containers have granted this exemption until 2014. Many factors, then, have to be taken into account, e.g. whether or not the exemption applies also to containers used not to ship goods but to store Grid or Cloud components. As often, a case-by-case analysis will be required.

Another possibility is to locate the Grid/Cloud datacentre in a marine off-shore structure, as Google is planning to do. The costs of implementing such a solution may be potentially huge, but also the benefits can be huge. In fact, in principle, we assume that the technology provider can escape from property tax, as, legally speaking, the datacentre is not located on any land, and from all other taxes. Basically the same problems are faced by oil and gas marine off-shore infrastructures: as a rule, if the building is inside the national waters of a specific country, the off-shore is deemed to be a permanent establishment of the oil and gas company. Therefore, the Grid/Cloud provider should locate the datacentres in international waters in order not to be subject to taxes, but this, of course, will imply very high costs and there is the eventuality that the solution cannot be implementable in practice.

### **3.2.2 Tips for end users**

Taxation affects primarily technology and service providers, and to a very limited extent end users. The area where end users play an important role is VAT, as they have to pay the tax when buying the services. Businesses then can offset the tax with the output VAT, but

consumers/end users simply have to pay VAT out of their pocket. As said above, it is not very feasible for a consumer to open an off-shore account to save VAT (it can be easy to do, but the benefits are not, usually, so big). This happens especially because a normal user can buy a lot of online services provided in a Grid or Cloud business scenario from providers located in Luxembourg. They still pay VAT, but the extra cost represented by the tax is no more than 15 %.

We should wonder what will happen as from the beginning of 2015, when the prices of e-services are expected to increase dramatically for many users in Europe. We strongly believe that this reform will have negative effects and will sustain the flourishing of companies providing fake locations for consumers. We can foresee, in fact, that many businesses operating at the borders between legality and illegality, or even in the illegality, will be created and they will sell online to European consumers the possibility to buy online services via an off-shore or a Luxembourgish bank account. It is not our duty to provide the reader with suggestions, probably many business people are already thinking about future solutions to make consumers' life easier.

### **3.3 Intellectual Property Rights**

IPRs are undoubtedly a very important issue in the field of the provision of Grid and Cloud services. A lot of effort during BEinGRID has been devoted to analyse which enablers and risks Grid/Cloud companies have to face in this field, and the results, in form of practical guidelines, can be summarised as follows.

#### **3.3.1 What about going open source? Licensing strategies**

First of all, technology and service providers must draft and implement a very careful IPRs strategy and policy. Breaching third party's rights can be expensive and may potentially limit or stop the development of the business concerned. A typical issue to assess regards the following question: going open source or not? Service providers are particularly affected by this issue, since, for what concerns Grid/Cloud providers, there is a strong open source tradition. Nothing should be added here to what has been produced by BEinGRID in the field of Grid middleware. Things are more complex for service providers.

The tension between the interests of a single company and of the market as a whole, highlighted at the beginning of the project, still exists. However, now, after many months of research and work, we can express a more mature judgement. Grid is clearly evolving to Cloud computing, populated of several service providers built on top of the Cloud. This means that it should be easier and cheaper to run a business as software house. No big infrastructure is necessary, the product does not have to be packed and sent to the shops or delivered via mail to the clients, and no expensive marketing campaigns on the press are required. In other terms, fewer investments are necessary to develop and market software and applications. This may justify open source solutions. The software, delivered as a service, may be developed, run and host in the Grid/Cloud of a technology provider. For the customer is convenient to download it for free and eventually to pay for extra features and for assistance. Another source of revenue may come from advertisement displayed in the interface of the software. Many possibilities exist.

From the legal point of view, it has to be said that many open source licenses exist. Which one is the best has to be assessed on a case-by-case basis, taking into account the specificities of each computer programme and the relevant market. Interoperability is surely an important factor: if the software is used in combination with other applications, no problems of license incompatibility should arise. The developer has also to consider whether he wants to allow users to improve the software, if the software can be used for commercial purposes, etc. One point must be clear: open source licenses available in the market are like

standards. They are widely adopted because they are easy, or for many other reasons, but no developer is obliged to follow them (at least when we talk about licensing an original product that has not been sub-licensed to the developer). It can sound strange, but legally speaking there are no barriers to the possibility to draft a specific open source license, tailored to the needs of the parties. Often, maybe, this can be the best solution, if some issues are not successfully dealt with by the standard licenses.

Licenses are also relevant if third party software is used in the context of Grid or Cloud services. In this case, licensing issues between the owner of the programme and the technology provider (and, if necessary, other parties) have to be addressed, explicitly taking into account the intricacies of Grid or Cloud architectures (e.g. avoiding the 'per-CPU' licensing model).

### **3.3.2 Copyright issues: liabilities and third parties**

The technology provider, on the other side, processes, even if often without any active role (e.g. in case of hosting) copyrighted material of third parties. These third parties can be the end users, the service provider/client, and any other third party with whom the technology provider does not have any direct contractual connection. It has been said, also in the framework of BEinGRID, that every time copyrighted material (like software, or any other material that can be protected by copyright) moves from one Grid/Cloud component there is an electronic copying of the protected work. This means that the party who stores the material needs to acquire the permission of the copyright owner so that the material can be stored, copied and processed in the various Grid/Cloud components. This approach is surely very strict, and may be criticised. By way of analogy, we can assume that storing the copyrighted material in different Grid/Cloud components is similar to making a backup copy of the material. Furthermore, the Grid and the Cloud have to be seen as a unique infrastructure. The copyrighted material is stored in the Grid or in the Cloud as a whole, and we believe that the internal division of the infrastructure in components is not relevant.

However, this strict approach must be proposed to the readers, and it has to be remarked that it is surely safer to communicate to the copyright owner that the material will be stored or processed in a Grid or Cloud infrastructures and that (temporary) copies will be made, given the nature of the Grid or Cloud infrastructure. This implies, of course, that the user of the material knows that the material will be hosted in a Grid or Cloud infrastructure. The technology provider, thus, has to advertise that the material uploaded by the clients will be hosted and processed in a Grid or in a Cloud. It is difficult to imagine that a technology provider does not do that, but however, theoretically, this omission may imply liability for the Grid/Cloud supplier.

The owner of the copyrighted material can also be the service provider that needs computing capacity from a technology provider to store, host or develop the programme. If the software is the own intellectual creation of the service provider, the computer programme is, in principle, protected by copyright. This implies that confidentiality issues are pivotal: we suppose that a service provider that stores his software in the Grid or in the Cloud would not be happy to know that the software has been shared with other clients of the technology provider or that somebody wrote an article or a post in a blog expressing negative judgements about the programme. Confidentiality shall be regulated in the SLA or in a separate contract, usually a Non-disclosure agreement, signed between the technology provider and the service provider. Of course, confidentiality is relevant in all relationships between a Grid/Cloud provider and a client. We assume that a person that stores pictures in the Grid/Cloud does not want to see them used for other purposes or to read nasty comments about them.

In practice, it is very unlikely that big technology providers sign every time a separate Non-

disclosure agreement with all their customers. Only important clients will have this privilege, the others have to rely on the provisions (if any) in the SLA. As said above, very often these clauses are provider-oriented and no big protection is granted to the customer. We strongly recommend technology provider to commit themselves to respect the confidentiality of all information stored in their datacentres, so that the customer is protected against any unwanted use of the material stored in the Grid or in the Cloud.

At the same time, it has to be clearly written in the SLA, or in another contract, who is the owner of what. In other words, the fact that data, files, software, etc are stored in the infrastructure of the technology provider shall not imply any transfer of ownership of the material. The term 'ownership' must be interpreted in a flexible way: we mean the right of ownership in the traditional sense (when applicable), the copyright, patent right, etc. So, the service provider who runs software or an application in a Grid or Cloud infrastructure keeps his rights over the software or application. The same applies to the user who stores files in the Grid or in the Cloud. It is common practice that this point is written in the SLA between the technology provider and the client. If not, the client should not trust the Grid or Cloud provider and should not buy services from him. The risk to lose data or material may be high.

### **3.3.3 Patentability issues and risks of infringing existing patents**

An important aspect of IPRs regards patents and patentability issues. Technology providers and software providers should verify respectively whether or not the innovations created by them can be granted a patent. The issue of patentability of software and of Grid/Cloud middleware and hardware components has been deeply analysed during the project. To the ends of these pages, the issue and risks of infringing existing patents is extremely interesting. A typical example is that of the service provider that offers a SaaS. Software, in principle, is not patentable in Europe, but there is the possibility that the same programme is protected by a patent in another country outside the EU. If this software is sold in the country where the patent has been granted, there is a patent infringement and the service provider may be held liable.

Of course, if the software must be stored in a CD and sold in shops, it is easy to avoid any patent infringement. Simply the software will not be sold or distributed in that country. But this possibility does not exist if the software is marketed online and can be downloaded by any customer. Or, at least, some measures have to be taken in order to avoid any trouble. These measures imply a limitation of the markets where the software is sold, typically (the list is not exhaustive):

- The software provider publishes a disclaimer in the website from where the software can be downloaded and declares that users from certain countries cannot download and use the software. Of course, it is not possible to impede that somebody downloads the programme against the will of the provider, but at least the latter will not be held liable;
- The software provider impedes, through a GeoIP system, that users from the country where the patent has been granted have access to the website and download the software;
- Payment for the software cannot be done with credit cards issued in the country where the patent has been granted. The system is not absolutely safe but statistically it will be effective and will prove that the service provider was aware of the risk of patent infringement and implemented measures to avoid it.

It is therefore necessary that the service provider performs a detailed investigation about potential patent infringements. The same research has to be done in order to assess whether the application is patentable or not (prior art research): since the invention must be new, the

same product cannot be already in the market. If this is the case in point, there is risk of patent infringements.

### 3.4 Data Protection and Security

Applicable European and national data protection regulations and principles must be taken into serious consideration in a Grid/Cloud computing scenario in order to avoid litigation with privacy authorities and fines. The logic behind some particular privacy rules may be hard to understand for business people (and not only), but nobody can neglect these regulations, that affect both technology providers and service providers. Security issues are also pivotal.

#### 3.4.1 Data protection in Grid and Cloud computing scenarios: what to do?

First of all, the importance of a privacy policy that regulates the relations between (i) the technology provider and the end user, and (ii) the technology provider, the service provider and the end user must be stressed out. This privacy policy shall clearly state the rules and responsibilities of the parties involved, and it plays a pivotal role especially when there are three parties involved (i.e. technology provider, service provider and end user). In a typical SaaS scenario, for instance, the end user will transfer data to the software provider (the service provider), but these data may be processed in the Grid/Cloud infrastructure of the technology provider.

In general terms, we can say that the service provider is the data controller (i.e. the party who determines the purposes of the processing of the data) while the technology provider is the data processor. In case of provision of Grid/Cloud computing and storage capacity directly to the end user, the technology provider will be the data controller. The reader must be aware that this distinction has to be analysed on a case-by-case basis, and the role of data controller and data processor may be attributed to one or the other party (the technology provider or the service provider) according to the concrete business scenario. In any case, what can the parties do with the data and how roles and liabilities will be split will be regulated by the privacy policy (together with a privacy agreement, if the two documents are not unified in one agreement).

Furthermore, the parties must verify which data can be processed and which standards must be followed. First of all, only personal data are affected by data protection regulations, i.e. all data that, basically, refer to a physical person. So the name of a company is not a personal data, as well as an email address like [info@companyname.com](mailto:info@companyname.com). Conversely, all email addresses that refer to a specific employee, as well as to phone numbers, etc, are deemed to be personal data and therefore they are protected. Then, some data are labelled as sensitive, and they are further protected. Medical data, information about political or trade union affiliations, information about sexual orientation, etc are sensitive data. To make an example, a provider of software for e-health services used in a Grid/Cloud environment must be aware of the nature of the data processed and of which authorisations, if any, are necessary to process these data. It is also highly advisable that the data are made anonymous when transferred to the Grid/Cloud provider. If these data are incidentally used for other, illicit, purposes, the consequences can be potentially dramatic as well as the damages to be compensated by the technology provider and/or the service provider.

A suggestion that we feel giving is to avoid the collection of personal data unless absolutely necessary. It may be the case, for instance, that processing data about the employees' of a company is not necessary, and that generic company's email addresses are available and therefore can be registered and processed instead of persona data. This reduces risks and red tapes for the technology or service provider. Of course, very often this is not possible, a case-by-case analysis is necessary.

We have also to stress out the importance of the consent of the data owner (i.e. of the

person who submits the personal data). The entity who receives data from the data owner, either the technology provider or the service provider, needs to inform the data owner about what will happen to his data and he has to give consent to the processing of the data. The readers are encouraged to perceive that the data subject's consent should be closely related to the notion of data processing. It follows that a general and *a priori* consent taken in the beginning of a business relationship might not suffice for further processing of the user's data: in every upgrading of Grid/Cloud infrastructure, the processors involved should contemplate whether the specific upgrade changes the way in which personal data are processed (for example, different data are processed, there is a transfer of personal data between servers in different countries, more data are added to the Grid/Cloud databases, new processing techniques are implemented, a new "co-controller" is introduced, etc). More comments about this issue will be done in the next lines.

What emerges from the above comments is that it is necessary to inform the data owner that a Grid/Cloud computing infrastructure will be deployed to process his personal data. In case of business scenario that involves a service provider and a technology provider, we can say that there is outsourcing of the processing of the data. The end user/data owner must be informed of all these elements so that no surprises for him will arise. If he communicates some of his personal data to a SaaS provider, he is supposed to expect that the SaaS provider will keep the data inside his premises, and not that the data will be transferred and processed to a Grid or Cloud provider. This is valid unless he is duly informed and he can decide whether or not to communicate his data to the SaaS provider.

Furthermore, the data owner must be able to modify or rectify his data at any time during the relationship with the technology or service provider. Things may change and it is in the interest of both parties that the information is accurate and up-to-date. Modification can be done by the data owner directly online or via a dedicated hotline (or with other modalities), but it has to be assured that the modification of the data is done by the person authorised to do so. We do not say that the use of a digital signature is required, in practice this would seem unnecessary in most business relationships, but a system of username/password is surely advisable. The application of data protection regulations has to be accomplished in a rational way, without undue care but with a high standard of care. The golden rule is: no panic! The technology or service provider mainly shall avoid any dissemination of personal data that is not strictly necessary to reach the business goals of the relation with the end user and according to the applicable rules and to what has been communicated to the end user. If this does not happen, privacy authorities may start investigations and impose fines to the infringer. This is, of course, a cost and may potentially damage the reputation of the company. In the era of ICT information travels very fast, and a company can be labelled as 'privacy-unfriendly' very easily. It is not necessary to highlight that many clients, sensitive about privacy issues, will never buy services from that enterprise.

This implies that privacy does not have to be taken into account only after the data are collected and risks are potentially behind the corner. In other words compliance to data protection legislation is better and more easily achieved when the applicable principles, explained above, are taken into consideration early in the development process ('privacy by design'). This can represent a cost, in terms of money and time, during the start-up phase, but it will surely reduce the costs for sanctions and costs linked to the bad reputation acquired by the company. Compliance costs are not risible, but sanctions can be much higher.

The principles not to forget in the development process are the following:

1. Fair and lawful processing;
2. Data controllers must obtain data only for specified and legitimate purposes, and

must not carry out any further processing which is incompatible with those purposes;

3. The data controller shall hold only personal data that is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
4. All personal data shall be accurate and, where necessary, kept up to date;
5. Personal data shall not be kept for longer than it is necessary for the purposes for which these data were collected;
6. Processing shall be carried out in accordance with the rights of the data subjects. More precisely, the applicable legislation grants data subjects the right to obtain certain basic information from the data controller about the processing of their personal data;
7. The issue of data security must be addressed as well and the applicable European sources require data controllers to take “appropriate technical and organizational measures” against unauthorized or unlawful processing, and accidental loss, destruction or damage to the data;

Furthermore, personal data must not be transferred to a country or territory outside the European Economic Area (that is, the Member States of the EU plus Norway, Iceland and Liechtenstein), unless that country or territory has in place a legal system that “ensures an adequate level of protection”. Please be aware that if the data controller makes the data run in a Grid or Cloud infrastructure located partially outside the EU, we cannot say that more data controllers are involved, and the same applies in case of a Grid or Cloud entirely placed in Europe. As far as only one legal entity manages the processing of data, it is possible to talk of only one data controller. This means that the place where the Grid or Cloud components are located is not relevant, as far as the technology provider is a European company. Different interpretations can be supported as well, but we prefer saying that the criterion to take into account is the place where the company is formally domiciled (basically registered).

The problem is likely to arise in all scenarios involving a service provider and a technology provider. An example will illustrate the point: client A, who lives in Belgium, communicates his data to the SaaS service provider B, established in Germany. B runs the SaaS on the Grid provided by company C, technology provider based in the Netherlands. C has Grid components in Russia, so potentially the data of A will be transferred to the servers located in Russia. In this case, we assume that there is no transfer of data outside the European Economic Area because the technology provider is a Dutch company. To avoid doubts and uncertainties, it is advisable that the service provider contacts the privacy authority of his country and asks for advice. This procedure is for free or at very low costs and confers legal certainty.

### **3.4.2 Security issues: legal approach and tips**

In a Grid or Cloud architecture, security is probably the most sensitive topic. We would say that real security must be differentiated from security perceived by the user. In other words, we are pretty sure that the real level of security existing in a Grid or Cloud environment is different from what the user believes. We mentioned before the importance of security in the SLA between the technology provider and the end user and/or the service provider. If we take into account the fact that the Grid/Cloud supplier very often in the market reduces dramatically or excludes any liability in case of security failures, we could conclude that they do so because it is impossible to ensure that no data will not get lost or damaged. In other words, the level of security is not yet optimal.

We cannot develop further technical considerations as we lack the necessary knowledge. But we can say that technology providers should align the level of security really implemented with the liabilities they assume in the SLA, i.e. with the level of security perceived by the user. We have to be honest: no legal or business consultant will recommend a client to store his data or to outsource the storing of sensitive information to a technology provider that wants to be always exempted from liabilities. Even if the security level of the provider is perfect, the client is not in the position to realise and appreciate that. Technology providers shall take some risks and let customers trust them. More generally, the feeling of the author, matured in the months of BEinGRID, is that the fear of security failures by users is the big threat to the full development of Grid and Cloud technology. Social networks built on top of the Cloud proved so far to be successful but we do not have to forget that users normally do not pay for using the service and at the end, even if many social scientists and economists say the opposite, they do not attribute too much importance to them.

Things are different when users pay for the service and they use these services to carry out their professional activities. Hosting in the Cloud sensitive information about a company or making complicated simulations in a SaaS environment is different than displaying a picture of the last holidays or posting a message directed to a nice lady. In the former case the risk is that if the data get lost or if somebody copies illegally the results of the simulations the company can go out of business. The risk is huge: if and how it can be avoided is the big challenge to allow Grid and Cloud computing to really change the ICT as we know it now.

### **3.5 The complexity of the Grid and Cloud business from the legal point of view**

Legal issues to be taken into account by who wants to start a business in the Grid and Cloud domain are not limited to those listed above. The first issue to analyse is about who is going to enter into the market. An ICT multinational willing to provide Grid or Cloud services usually has already the experience and maturity to cope with all corporate aspects. Things are different for a small start-up attracted by the possibility to make money following the paradigm of “everything as a service”.

Then, the market targeted by the provider is also pivotal. B2B radically differs from B2C, as we said above. B2B generally has fewer risks than B2C due to the existence, in the latter case, of many rules aimed to protect consumers. However, even in B2B, many sector-specific and local regulations must be taken into account. To make an example, A (technology provider established in Italy) wants to make a partnership agreement with B (service provider established in Belgium) in order to provide services under the common brand of A. If the contract is regulated by Belgian law, the draft of the partnership agreement, together with a document explaining the rights and obligations of both parties and other issues, must be sent by A to B at least one month before the signing of the contract. If this requisite is not met, the agreement can be declared void by a judge under request of B.

If, conversely, the agreement will be regulated by Italian law, this requisite does not apply, and there is no prior information obligation for A. Both countries are part of the EU, but they follow completely different rules as regards partnership agreements.

Furthermore, Grid and Cloud businesses have to follow sector-specific regulations, like in the financial sector. In this case, attention should be paid to the place where the company is established and to the place where the Grid/Cloud components are located. It may be the case in point that the national financial market regulator wants to know where the financial data are processed (for instance, in case of outsourcing by a bank or another financial institution). The Grid or the Cloud, of course, cannot become ways to avoid controls by

market regulators. This can happen especially in case of sub-contracting of business functions to several technology providers acting in a cooperative way such as to make, de facto, a Grid or a Cloud. What we say is maybe futuristic, but theoretically (and we believe, also practically) it is possible to create ad hoc Grids of Clouds that act as 'grey areas' where control become difficult or impossible.

We do believe that the location of the Grid and Cloud components shall be always clearly disclosed by the technology provider. The clients (and when applicable, public regulators) have the right to know where the data are stored or processed. This consideration is extremely important also in the area of criminal law: the risk is that the Grid and the Cloud become an extraterritorial entity where no jurisdiction applies. With this regard, basically three solutions/approaches apply:

1. The laws and regulations of the country where the Grid/Cloud components are located apply: given the nature of the Grid and Cloud, this principle is difficult to apply. An example will clarify this issue: person A, living in Europe, posts online messages promoting terrorism against Europe using the services of company B, whose servers are located in countries that, officially or unofficially, support international terrorism. Is it acceptable that A cannot be sentenced in Europe because the messages are hosted in countries where promoting terrorism is not a crime?
2. The laws and regulations of the country where the Grid/Cloud provider or service provider is established apply: the same considerations developed above apply. This system would simply motivate companies to be resident in countries with insufficient or weak legislation in order to avoid any and all risks.
3. The laws and regulations of the country where the service is accessible or of the country targeted by the provider apply: this is probably the best rule to follow, but at the same time it means that technology and service providers are subject to an incredibly high number of laws and regulations. As usual, a balance has to be found: we assume that it is better if many rules apply rather than if no rules apply. If a technology or service provider wants to target several countries, he has to respect the laws locally applicable. In a positive way, this means that (in the example under no. 1) person A can be prosecuted in Europe since promoting international terrorism may be a crime, but, at the same time and in a negative way, undemocratic countries are allowed to impose filters and censorships to foreign technology and service providers if the services are accessible from those countries.

The trend that sometimes emerges is that big technology and service providers want to impose their laws. An interesting case reported by the press <sup>1</sup> indicates this tendency. Recently Google communicated to the office of the prosecutor of Milan, Italy, that, even in case of criminal investigations in a foreign jurisdiction (like in Italy), Google reserves the right to decide which data can be transmitted to the police and to the prosecutor and also the right to establish for how long users' data can be stored in the servers. This applies also in case of urgent life danger for people (e.g. if a kidnapper sends a message to the family of the victim asking for money using a Google mail or messaging service).

This shows that ICT providers, sometimes, pretend to be above any laws and to make themselves laws. We can understand, to a certain extent, the position of Google. Since the

---

<sup>1</sup> See [http://www.corriere.it/cronache/09\\_settembre\\_28/pm\\_contro\\_google\\_dati\\_luigi\\_ferrarella\\_6e06f990-abfc-11de-8068-00144f02aabc.shtml](http://www.corriere.it/cronache/09_settembre_28/pm_contro_google_dati_luigi_ferrarella_6e06f990-abfc-11de-8068-00144f02aabc.shtml).

Grid/Cloud components they use are located everywhere in the world, and at the same time they are intended to provide services worldwide, it is of course difficult to imagine that Google must be forced to respect the legislation (regarding, for instance, the period of compulsory storing of information) of all the countries of the world. The only feasible solution would be, of course, that Google stores all data forever, but in this case there is the risk to infringe the legislation of many countries that set a maximum period of time for storing data!

We can say that no univocal solution exists. ICT is faster than law and policymakers and it is, by its nature, global, while laws and regulations are often merely national. In the above example from Italy, the prosecutor reasons as if Google is only obliged to follow Italian law, but Google is a global company with operations everywhere. Given the economic power of the company, there is at the same time the risk that Google pretends to make the rules for itself, which is absolutely dangerous and not democratic. At the same time, for many service providers that do not have the power of Google respecting all existing laws and regulations at worldwide level is simply a cost that they cannot sustain.

Is there any feasible solution? Who is going to win the match? National authorities, representing the power of a State, or ICT companies that need flexibility and, at the end, lack of rules? The answer to these questions is extremely cumbersome. Probably the difficult balance existing now between States and ICT providers will go on for many years. Sometimes they are allies, sometimes they discuss or argue, but in general they have to find a balance between different interests. States must understand that it is not reasonable to ask companies to follow too many rules. Companies have to understand that they cannot be immune from laws. The future will tell us if there is a winner.

## 4. Conclusions: check lists for technology providers and service providers

### 4.1 Legal issues are not enough: check list for technology providers

We are at the end of the last legal Deliverable of BEinGRID. This project was undoubtedly an amazing experience, first of all because it allowed the author of these pages to discover several fascinating legal, technical and business issues. Grid and Cloud computing paves the way to new problems faced, first of all, by technology and service providers. Grid and Cloud is by its nature international: we believe in the paradigm of resources located in different countries that are interconnected and work in a cooperative way. This is the very challenge of dispersed computing: going beyond national borders and offer solutions to as many customers as possible. Locating computing resources in only one country renders more difficult and expensive the provision of services to customers located in other continents: Grid and Cloud computing, in this sense, should open the doors to new business attitudes, more globalised and international.

Many challenges, of course, have to be tackled. Interconnection of resources in different countries or continents requires better telecommunications connections, especially to locate Grid/Cloud components and provide services in countries under development. Without good network connections no international Grid or Cloud can be implemented. But technical barriers are not the only ones: in the course of the project we found out several legal barriers, i.e. legal aspects that render the implementation of transnational Grids or Clouds difficult. These issues affect especially technology providers: when connecting resources as to create a Grid or a Cloud, these companies shall really wonder whether this would be feasible from the legal point of view and where the components should be located. From the legal point of view, some countries are better than others, although it is not possible to make general statements. At the end, very often, cultural elements have to be taken into account as well, like the familiarity with national laws, relationships with the personnel, etc. An example will clarify this point: a technology provider established in Norway can wonder whether or not France is a good place to locate the Grid/Cloud components. From many points of view, maybe France is better than Norway, but if we consider that the management of the technology provider has to get used to different legal rules, to negotiate with trade unions that are radically different from those in Norway, to deal with public authorities that have a different attitude and mentality than in Norway, etc, we see that maybe there are more disadvantages than advantages.

In other words, legal considerations are not enough. A careful legal and tax planning must consider also cultural and political aspects. The main questions that a technology provider has to analyse when assessing where Grid/Cloud components should be located are the following (please be aware that the list is not exhaustive):

- *If the technology provider wants to open a subsidiary that manages the Grid/Cloud infrastructure, which legal form does it have? Where is it better to incorporate the subsidiary?* Often there is no objective need to open a subsidiary that manages the ICT resources, but sometimes tax (or other) reasons make this solution feasible and advisable. Usually the subsidiary will have the form of a company with separate capital and liability from the shareholders and therefore it is necessary to see which country is more attractive for this kind of investments (e.g., to assess the rules about minimum capital requirements, involvement of workers and other stakeholders in the management of the company, rules about deductibility of losses, etc).

- *How many taxes have to be paid on the profits generated by the Grid/Cloud?* Tax considerations have been developed above: taxation is undoubtedly pivotal and technology providers shall implement tax planning strategies. See above for further comments.
- *What about the people working in the datacentres?* Employment law issues shall not be neglected. The technology provider can employ ad hoc personnel for the Grid/Cloud components located in other countries or can second its personnel to these datacentres. In the former case, the company has to assess the cost of labour, if it is necessary to employ people or if they can be recruited on the basis of a collaboration contract (thus working as self-employed, and to what extent this possibility is feasible), how many social security charges must be paid, etc. In the latter situation, the conditions for secondment of workers applicable in the country where the technology provider is established and where the workers have been employed must be analysed.
- *What about the general legal environment of the country?* With the expression 'legal environment' we mean several elements, like the efficiency of the judicial system, the level of complexity of the applicable legislation, the flexibility and efficiency of public administration, etc. If disputes arise, and have to be treated in the country where the Grid/Cloud component is located, the legal environment is extremely important.

## **4.2 Service providers: to what extent are they dependent on technology providers?**

Service providers face issues that are partially different from those listed above. Companies providing services on top of a Grid/Cloud infrastructure owned and managed by a technology provider do not need, in fact, datacentres or other ICT infrastructures, but they have to deal with other legal and business issues. The most important aspect that they have to assess is: to what extent do they want to be dependent on technology providers? Often, in fact, service providers are subsidiary of technology providers, and at the end many companies operate as service providers and as technology providers at the same time. Google, for instance, owns and manages datacentres and provides services to clients; Amazon does the same, but at the same time it operates as technology provider for other companies that provide other services to customers.

The problem exists when the technology and the service suppliers are two completely independent entities: they can be independent from the corporate law point of view, as there is no relation of control or any other link between the two entities. However, de facto, and from the business point of view, the situation may be more complex. If a service provider buys computing or storage capacity from a technology provider in order to deliver services to customers, in practice the former depends on the Grid/Cloud provider. The content of the SLA usually imposed by big international technology providers (see above for further considerations) justifies our statement: the service provider is expected to trust the Grid/Cloud supplier and if something goes wrong, the consequences will be sustained by the service provider.

In other words, the de facto absence of liability for the technology provider creates forms of substantial dependency that are not contemplated by corporate law. And the service provider must assess whether or not he wants to accept this dependency knowing that, very often, there are no alternatives, at least until the number of commercial Grid/Cloud providers is limited and there is no real competition in the market. Or until the policymaker (we think especially about the European Commission) intervenes and asks technology providers, even if they are based in other continents, to apply fair contractual provisions.

Actually there are no legal grounds for that, but soft law mechanisms can be more efficient (and easier to implement) than traditional legislation. Between the many possible solutions, we would suggest the creation of a label for technology providers that apply fair contractual provisions (mainly in the SLAs with customers). The Commission could promote the setting up of an independent consortium, composed of academics, consumers' representatives, etc who has the task to evaluate the content of the contracts imposed by technology providers. If they are user-friendly, a label of 'good practices' can be issued, so that the company can display it in its website and in the marketing campaigns. This system, if duly promoted and implemented, can stimulate ICT companies to improve the fairness of their contracts and, ultimately, to invest more in innovations with the aim to render the clients as satisfied as possible.

## Annex A. License conditions.

This is a public deliverable that is provided to the community under the license Attribution-NoDerivs 2.5 defined by creative commons <http://www.creativecommons.org>

### This license allows you to

to copy, distribute, display, and perform the work

to make commercial use of the work

### Under the following conditions:



**Attribution.** You must attribute the work by indicating that this work originated from the IST-BEInGRID project and has been partially funded by the European Commission under contract number IST - 034702



**No Derivative Works.** You may not alter, transform, or build upon this work without explicit permission of the consortium

For any reuse or distribution, you must make clear to others the license terms of this work.

Any of these conditions can be waived if you get permission from the copyright holder.

### This is a human-readable summary of the Legal Code below:

#### License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

#### 1. Definitions

**"Collective Work"** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.

**"Derivative Work"** means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

**"Licensor"** means all partners of the BEInGRID consortium that have participated in the production of this text

**"Original Author"** means the individual or entity who created the Work.

**"Work"** means the copyrightable work of authorship offered under the terms of this License.

**"You"** means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

**2. Fair Use Rights.** Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

**3. License Grant.** Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works.

For the avoidance of doubt, where the work is a musical composition:

**Performance Royalties Under Blanket Licenses.** Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g.

webcast) of the Work.

**Mechanical Rights and Statutory Royalties.** Licensor waives the exclusive right to collect, whether individually or via a music rights society or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

**Webcasting Rights and Statutory Royalties.** For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Derivative Works. All rights not expressly granted by Licensor are hereby reserved.

**4. Restrictions.** The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any credit as required by clause 4(b), as requested.

If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or Collective Works, You must keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or (ii) if the Original Author and/or Licensor designate another party or parties (e.g. a sponsor institute, publishing entity, journal) for attribution in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; the title of the Work if supplied; and to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

**5. Representations, Warranties and Disclaimer.** UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE MATERIALS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

**6. Limitation on Liability.** EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### **7. Termination**

This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

#### **8. Miscellaneous**

Each time You distribute or publicly digitally perform the Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.