COUNCIL OF THE EUROPEAN UNION

Brussels, 1 October 2012

14411/12
ADD 1

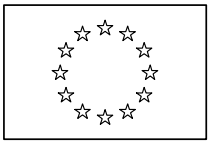
TELECOM 170
MI 586
DATAPROTECT 112
COMPET 585

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	27 September 2012
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	SWD(2012) 271 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Unleashing the Potential of Cloud Computing in Europe

Delegations will find attached Commission document SWD(2012) 271 final.

Encl.: SWD(2012) 271 final



EUROPEAN COMMISSION

Brussels, 27.9.2012
SWD(2012) 271 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEEE AND THE COMMITTEE OF THE REGIONS

Unleashing the Potential of Cloud Computing in Europe

{COM(2012) 529 final}

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEEE AND THE COMMITTEE OF THE REGIONS

Unleashing the Potential of Cloud Computing in Europe

1. INTRODUCTION

This Staff Working Paper provides supporting analysis to the political proposals in the Cloud Strategy Communication (COM(2012)529). The document is presented in six sections. The first section considers of key definitions of cloud computing and discusses why it is of major policy interest. The second section looks at the energy and environmental impacts of cloud computing. The third section provides an analysis of the emerging demand for cloud computing in terms of its potential growth as a sub sector of the ICT industry but also the factors conditioning its take up and use in the key demand areas of large and small enterprises, the public sector and consumers. The section draws heavily upon the results of a survey commissioned by the European Commission to investigate factors of demand. The fourth section reports on the key results of the consultation that has been carried out to investigate users viewpoints. Section five looks in more detail at the various areas of the Digital Agenda (in particular the chapter on the Digital Single Market) and its relation with cloud computing services. The sixth section presents specific key actions on cloud computing.

2. DEFINITIONS – WHAT IS CLOUD COMPUTING AND WHAT ARE THE MAIN POLICY CHALLENGES?

The economic figures reported below indicate that cloud computing has substantial economic potential. First cloud computing reduces the overheads of operating computer systems. Second considerable gains are also likely from service innovations and the adoption of new organisational processes that increase efficiency.

To understand these changes it is necessary to first to understand what cloud computing is. The basic essence of cloud computing is the provision of "utility computing".Of the various definitions in use the most widely accepted appears to be the one put forward by NIST in 2009:

> Cloud computing is a model for enabling convenient on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [1]

[1] NIST (2009) Cloud computing definition, updated by NIST (2011) SP 800-145 US National Institute of Standards and Technology

This definition stresses the technological configuration of cloud computing, which however may be less important than the changes that it brings. By viewing cloud as a business model the accent can be placed on the key business process characteristics of cloud computing such as:[2]

- Users do not need to invest in their own infrastructures, storage and processing takes place in the cloud rather than at the users premises or on the user devices
- Cloud services can rapidly scale up or down according to demand
- Cloud virtualises computational power so that the physical location of users or computer resources are no longer a constraint
- Computing becomes an operating rather than a capital expenditure item

These are all features that differentiate cloud computing from data centre outsourcing. It gives scale: the "illusion of unlimited resources." But it also signals a loss of control as users become reliant upon leased line or public broadband connections and upon the distributed computer systems of the cloud provider. This also distinguishes cloud from grid computing, which does not emphasize this external centralized control but rather the sharing of networked computing resources.

The mode of provision therefore is crucial to understanding the impact of cloud computing: first it is primarily an economic phenomenon rather than a technological one. The external provisioning of computing as an on-demand service that uses virtualisation (e.g. running several logical servers on the same physical hardware) and optimises data and processing loads across more than one physical site (across an array of data centres) means that in principle, from a technical point of view, neither the data owner nor the processor need to know where the data is residing.

The cost efficiencies of the cloud stem from aggregating peaks and troughs of demand across a large set of customers. This is in fact how cloud technologies first took off because major eCommerce providers (e.g. Amazon) tried to increase the utilisation of their own facilities by leasing capacity in their data centres to clients that had different usage patterns. Larger and more diverse populations (geographically and in terms of use patterns) can be served more cost efficiently than smaller or more homogenous populations. The cost reduction comes from offering economies of scale of service above that which the individual user organisation can afford or would need.

However, for many users letting-go of explicit knowledge of data location or sharing data centres with other users is problematic. Typically they are faced with compliance obligations related to the protection of sensitive data (e.g. personal data covered by data protection rules, commercially sensitive data or data which is of national strategic importance such as defense or police information). Thus cloud providers have been developing solutions to uniquely and dynamically reconfigure the data storage and processing to meet these requirements.

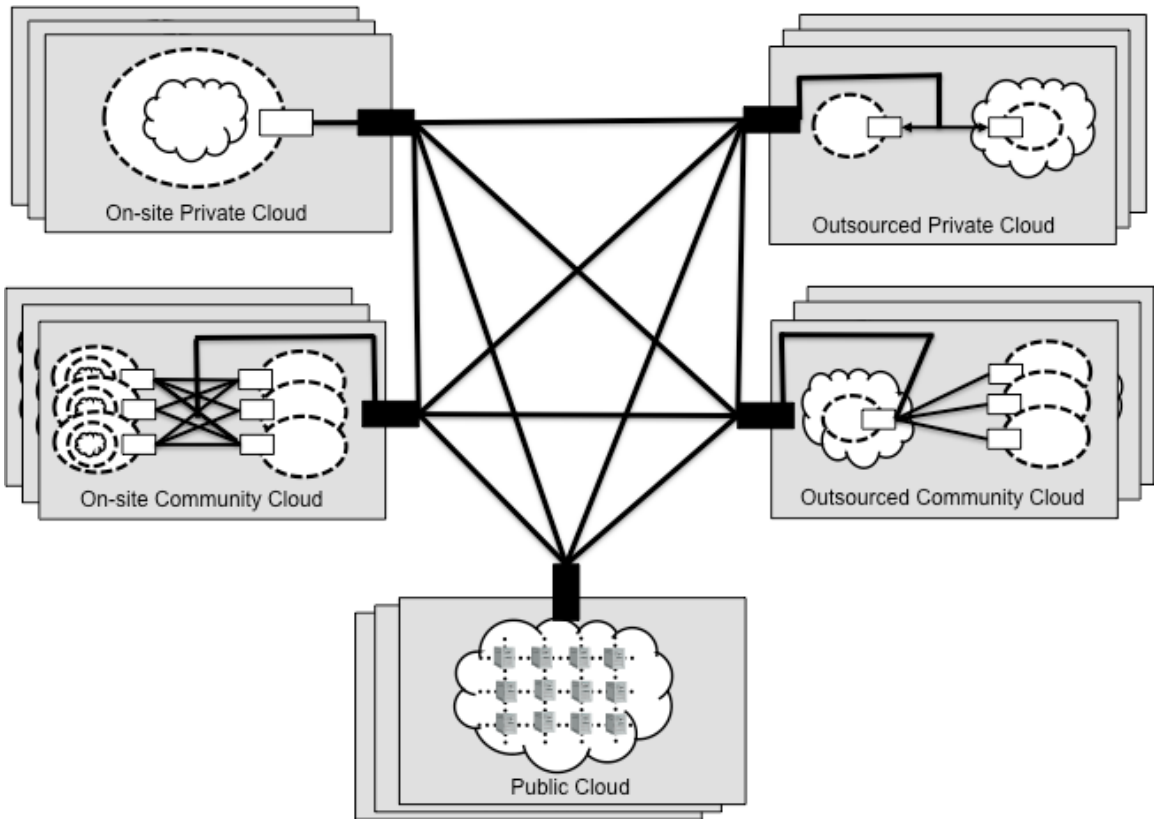
While often now thought in terms of the provision of access to data centre (infrastructure as a service or IaaS), cloud provision actually started in the form of the offer of platforms which

[2] Kushida et al (2012) The Gathering Storm: Analyzing the Cloud Computing Ecosystem and Implications for Public Policy, Communications and Strategies, 85:63-85

customers could use to process data from of for their clients (platform as a service or PaaS). For example Salesforce began by offering customer relationship management services to business clients on leased data centres of an IaaS provider. The offer of software as a service e.g. the direct provisioning of end user services such as email or social networking sites (Software as a Service or SaaS) completes the vertical stack of service offers from the basic Infrastructure (IaaS) to Platform (PaaS) to Software Application (SaaS). Each layer in this stack can be run as an integrated or entirely disintermediated service. The cloud service provision is complex and interdependent and it is not always clear to the user who is who in the chain of sub-providers of cloud services and how the different roles and responsibilities are assigned. Moreover, the place of establishment of these organisations may not always be apparent, thus raising questions of applicable law.

In addition to this multi-layer characteristic of cloud computing services, there are also different degrees of use of public or shared IT resources. In this respect, cloud is sometimes seen as a continuum (see Figure 1). Starting from traditional dedicated and in house IT resources which are operated by internal teams, a move towards the outsourcing of the operational management and/or the physical location of the data facilities can be seen as an antecedent to cloud computing as it implies a handing over of direct control to a third party under rather specific contract conditions (service level agreements). Cloud computing proper starts once there is use of virtualisation technologies to share, and thus raise the efficiency of IT resources. As a result various different deployment models for cloud computing are emerging from completely private clouds (where computer use takes place inside a security perimeter) to fully public clouds (where the cloud services and IT resources are shared between all and any users). In between these two extremes there are intermediate concepts. Community clouds are where the IT resources - which could be on the users site or outsourced - are shared between a closed community. For example a multi-agency cloud service provided exclusively to government bodies. In hybrid clouds, part of the data is in a private space and part is hosted on a public service, combining several of the other types of cloud.

- Figure 1: An example of a Hybrid Cloud



- Source NIST (2012) SP 800-146

When the different layers of services (IaaS, PaaS, SaaS) are mapped onto these different models, data control issues become potentially quite complex[3]. The different possible configurations have different implications as regards user control and thus require awareness and conscious decisions about data flow through the cloud value chain. For example, the less exclusive the use of infrastructures the more demand there will be for effective isolation within the cloud as regards sensitive data.

3. ENERGY AND ENVIRONMENTAL CONSIDERATIONS AND THE CLOUD

The rapidly increasing energy and environmental footprint of the Internet:

The unprecedented increase of data flow and processing of information over the Internet has an important environmental impact notably in relation to energy and water consumption, and greenhouse gas (GHG) emissions.

Some indicative examples that appeared recently in the international media[4] are the following:

[3] See NIST (2012) Cloud Computing Synopsis and Recommendations, PS 800-146

[4] http://www.greenpeace.org/international/Global/international/publications/climate/2011/Cool%20IT/dirty-data-report-greenpeace.pdf
http://www.disinfo.com/2011/05/internet-uses-more-electricity-in-u-s-than-auto-industry/

- The Internet uses more electricity in America than the auto industry uses to make cars and trucks.

- The combined electricity demand of the Internet/cloud (data centres and telecommunications network) globally is 623bn kWh (and would rank 5th among countries).

- Based on current projections, the demand for electricity of the Internet/cloud will – in the next few years - more than triple to 1,973bn kWh, an amount greater than the combined total demands of France, Germany, Canada and Brazil.

The above figures (and taking into account that the cloud is becoming one of the most important - if not the dominant - service model over the Internet), clearly demonstrate the need to link cloud related public policies to the energy consumption and environmental footprint of the ICT-sector.

Energy and environmental sustainability and the cloud:

Among the main claims of cloud computing is that it potentially leads to significant energy savings due mainly to the fact that is based on the flexible and scalable use of IT-resources[5]. Large companies in the US could save $12.3 billion annually in energy consumption by adopting cloud computing, according to some estimates.[6] The complete environmental effect from the deployment of cloud computing, however, depends not only on the amount but also on the type of energy that is used (which in turn is directly related to the greenhouse gas (GHG) emissions). Coal, for example, is considered as having high GHG emissions.

The current situation concerning the environmental impact of cloud data centres that are aimed to provide cloud services is quite problematic. Important cloud service providers appear to be in a race to build new, or upgrade existing, data centres in order to be able to capture the largest possible part of the rapidly emerging cloud market for them. As recent reports reveal[7], however, many of those data centres are powered by (still cheap) energy from coal.

Ignoring the above environmental effect of the cloud would be a missed opportunity for Europe. Europe should not only be in the front line of the global competition to promote growth around clouds but should promote in parallel green growth, i.e. the EU's environmental and climate agenda, through the cloud.

Measuring the energy , water and carbon footprint of the cloud:

The starting point for any policy regarding the energy and environmental footprint of the cloud is the ability to reliably measure this footprint. The landscape in Europe and the world appeared until recently fragmented on that front (and this concerned not only the cloud-services sector but the whole ICT-sector). International consortia (or even individual

5 eg, http://www.microsoft.com/environment/cloud.aspx

6 http://www.broadbandcommission.org/net/broadband/Documents/bbcomm-climate-full-report-embargo.pdf

7 Eg, http://www.greenpeace.org/international/en/publications/Campaign-reports/Climate-Reports/How-Clean-is-Your-Cloud/

companies) were using and their own methods of measuring energy and environmental footprint.

The Commission took the initiative to a global level through a Recommendation of October 2009 (adopted later as a Digital Agenda Action) *on mobilising ICT to facilitate the transition to an energy-efficient, low-carbon economy*[8] to change the above landscape. The Recommendation notably called on the ICT industry to develop a framework to measure its energy and environmental performance and adopt common methodologies to this end by 2011.

In the context of the above initiative, the Commission:

- Has engaged in discussions with relevant standardisation fora (notably the ITU, ETSI and IEC) and international initiatives (notably the GeSI/Carbon Trust /WBCSD[9] one) with the objective to facilitate the development of relevant standards supporting the establishment of a common methodological framework within the deadlines of the Recommendation.

- Is supporting pilot tests by industry on standards resulting from the above standardisation fora/initiatives to further facilitate and accelerate the process of creation of such a common methodological framework[10].

- Integrating metrics for the energy consumption and GHG emissions of cloud services into the above mentioned ongoing standardisation work by the ICT sector, is possible and would be appropriate. An example of an important metric that is currently being used and that could be enhanced in the future, is the Power Usage Effectiveness (PUE) of data centres. The European cloud strategy will serve to link future cloud policy developments with the energy and environmental agenda of the EU. The Structure of Demand for Cloud Computing

3.1. The growth potential of cloud computing

The available studies on the potential for cloud computing to contribute to growth and jobs have mainly been sponsored by the IT industry:. so far there are few fully independent investigations of the economics of cloud. A sampling of these reports indicates that:

- The global market size is expected to rise steeply – from 21.5bnUSD (2010) to 73BnUSD in 2015 according to IDC,[11]

- Cloud computing will boost GDP by between 1 and 2% of GDP in Europe's biggest five economies.[12]

- Cost savings for adopting organisations will be in the range of 20 to 50% of ICT spend

- Cloud computing will add 11.3 million jobs to the worldwide economy by 2014.[13]

---

8 C(2009) 7604

9 http://www.gesi.org

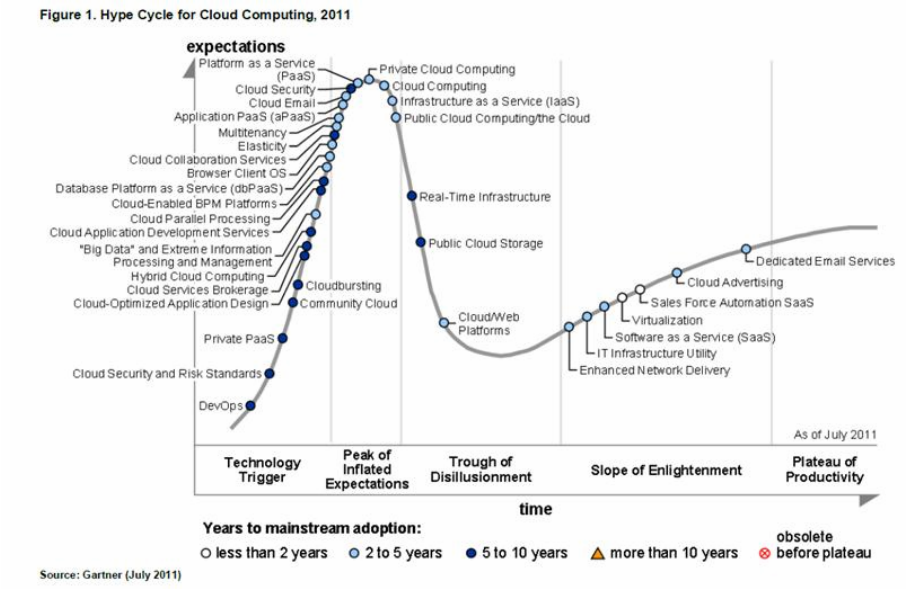
10 www.ict-footprint.eu

11 IDC (2011) Worldwide and regional public IT cloud services 2011-2015 forecast

12 Etro F (2011) The Economics of Cloud Computing

13 http://www.microsoft.com/presspass/download/features/2012/IDC_Cloud_jobs_White_Paper.pdf

Figure 2 – The Cloud Hype Cycle



In order to try to put these various findings into context the European Commission contracted IDC to undertake a survey of enterprises already using cloud computing. The objective of the study was:

To analyse the expected demand for cloud computing in Europe providing quantitative estimates. Since this demand is highly influenced by the policy context and the regulatory framework, it will also identify the main barriers to the take up of cloud computing in Europe by industry and consumers. Finally, it will propose recommendations for European policies and regulatory framework updates in order to accelerate the take up of cloud computing.[14]

The economic scenarios in this study indicate that public cloud computing could grow by an extra 33bn€ (to 78bn€) in the EU if appropriate policy action were taken to overcome barriers generating an extra 2.5 million jobs in the process.

The public cloud market (i.e. cloud services using servers that are shared between multiple users as opposed to being on dedicated private data centres) in the EU in 2011 reached €3.5 billion for software services and €1.1 billion for hardware services. Spending on cloud is thus still limited. Public cloud services accounted for just 1.6% of total IT spending in the business segment in 2011. But IDC's estimates indicate that on current trends by 2014 the EU public cloud services market will reach €11 billion in revenue, a compound growth rate of over 30% per year. Investment increases will be equally strong in public cloud software and public cloud hardware services (server and storage capacity as a service), across all vertical markets and company sizes.

At an overall level, this survey indicates that 97% of cloud users said they had made savings (typically in the range 10-20% of IT cost), including 36% who saw savings of 20% or more. Business benefits do not stop at cost savings. Users cite more effective mobile working, higher productivity, more use of standard processes, better ability to enter new business areas and the ability to open up in new locations as expected benefits.

[14] IDC (2012) Quantitative Estimtes of the Demand for Cloud Computing in European and the Likely Barriers to Take-up

Thus despite concerns that cloud computing may be overhyped (see Figure 2) there is strong evidence that there is already considerable economic potential from cloud to reduce costs and trigger innovation.

3.2. The cloud as a lead market

The EU market for cloud is some years behind the US market in terms of size and maturity. Most of the first wave cloud services vendors were US companies whose products were and remain orientated towards the US market. Vendors are addressing this problem by diversifying their offer.

The most important constraints on the growth of cloud in Europe relate to concerns by both suppliers and users about compliance with regulatory obligations. They sometimes have to comply with different national law and that such compliance is uncertain and costly. According to the IDC study undertaken for the Commission, removing some of the most serious differences between the Member States is regarded as helpful to secure scale efficient and cross borders cloud offer and use.

Considering first at cloud-based provision of IT infrastructures, it is argued by some observers that although experiencing very dynamic growth the IaaS layer is already consolidating and around a few leading heavy investors – data centres are capital intensive - all of them US headquartered notably Amazon-EC2, Microsoft Azure and RackSpace. In this process the IaaS is becoming a commodity (i.e. utility computing) where switching costs are relatively low.[15] This perspective argues that the value growth of cloud is higher in other parts of the cloud value chain – in particular the provisions of PaaS and SaaS, which are expected to represent 60-80% of the cloud revenues in the coming years. Moreover, entry barriers to these segments of the cloud market are lower, because of lower capital investment required and also because these are for the moment emerging markets. European-based players potentially have an edge in these layers because of existing strong systems integrators and business process consultants (e.g. Atos, Cap Gemini, Orange Business Services, SAP and TS Systems) that are accustomed to delivering services to diverse market segments, and have competitive strengths in trust, security and data protection and a familiarity of working in collaborative partnerships with other suppliers, which is expected to be a feature of the cloud ecosystem.[16]

3.3. Cloud take up in the private sector

A majority of firms in Europe (64%) are already using cloud services but as noted above spending is still limited because firms are cautious about adopting cloud services. Mostly firms are still trialling cloud services by adopting a limited set of non-business critical services. This reduces risks but also reduces the potential economic gains from cloud computing adoption.

In terms of growth drivers, larger firms (>250 employees) are expected to dominate cloud related expenditure in the coming years, growing from 81.5% in 2011 to 84% by 2014. SMEs will however be showing considerable expansion, with annual growth rates above 20%.

---

15 Forrester (2011) Sizing the Cloud, see www.forrester.com/Sizing+The+Cloud/fulltext

16 For an elaboration of this argument Rossbach C & Welz B (2011) the Survival of the Fittest, Roland Berger and SAP

As regards patterns of adoption, overall, European firms are smaller and show more conservative attitudes towards IT in general and cloud in particular. They seek measures to reassure themselves that cloud is "safe" for them, for example by waiting for governments to lead by example in cloud adoption. This caution is reflected in an incremental pathway of adoption of cloud. Firms generally start by adopting one cloud service then extend adoption to further applications once they have seen success. The main factors behind this caution relate to worries about applicable law and jurisdiction, security and data protection with respect to cloud services. For this reason most cloud developments in Europe are in dedicated private clouds, which are more legally predictable and secure but do not offer such high economies of scale as fully shared public clouds. So far, there is not much concern amongst firms about portability of data or vendor lock-in. In fact, respondents to the IDC survey indicate that conventional IT services may create greater lock-in because they involve investments into physical installations. Lock-in may however become more of an issue as the market matures and as the degree of dependence on cloud provision grows. This conclusion is corroborated by responses to the survey and may be nearer at hand than is sometimes appreciated, as already today around 70% of organisations using the cloud use multiple cloud services, and the average number of cloud services used by this group is just over five. Also, organisations that use the cloud expect to see further benefits beyond those they have already seen, in particular in productivity gains, standardisation of processes, exploiting new business opportunities, and increasing business volume.

The IDC survey indicates markedly different dynamics between larger enterprises and mid-sized firms on the one hand and micro firms (<10 employees) on the other. Larger firms are expecting to see major business benefits across the board from: mobile working (80%), productivity gains (80%), generation of new business (75%) standardisation of business process (75%), a release of capital expenditure from IT spend into other areas of spending (70%), an increase in business volume (70%) and easier set up of branches in new locations (70%). Cloud provision, however, has so far delivered on these expectations for only about 20-30% of respondents. Business benefits also seem to take place once the firm is fully engaging in "cloud-sourcing" across the whole range of IT systems.

Non-adopting firms are mainly concerned about data protection, data breach risks, liability of cloud providers, guarantees that the services will be up and running all the time, confidence in authentication and e-identification tools and dispute resolution. Concerns about jurisdiction under which these concerns might have to be addressed were also a consistent concern.

Micro enterprises of 1-9 employees have the lowest adoption rates of all firms despite having potentially much to gain in terms of on-demand access to scalable, state of the art informatics services. However micro-enterprises do not see it that way. The survey indicates that the cloud does not provide them with cost savings (only 11% of them report cost reductions) or tangible business benefits. According to IDC this apparent contradiction stems from the fact that cloud services have not yet emerged that are tailored to the needs of this market segment. Indeed smaller firms that do adopt cloud are typically attracted by "free" services

For smaller firms (and indeed consumers) the lack of availability of reasonably priced, reliable broadband connections is still a barrier. Though increasingly cloud services (and especially applications) can be accessed via mobile devices, this is still an issue for other types of service. Encouraging better broadband access especially for small and mid-sized businesses should improve adoption.

3.4. Cloud take up by the public sector

The take up of cloud by the public sector is subject to the same concerns as seen amongst large private organisations: how to maximise cost saving and service value from the cloud, how suitable are the business processes and existing systems for cloud provisioning, how can data be made safe in the cloud (as regards confidentiality, integrity and availability), how to determine the best contract models (or service level agreements), how to manage the transition from legacy systems to cloud systems and how to avoid lock-in to proprietary systems.

The big attraction of cloud for the public sector – especially at this time of austerity – is the prospect of major cost savings. This is evident from the various strategies that have been adopted by governments in Europe and beyond to overcome these concerns. Notable amongst these are the Cloud First Strategy of the US government, while in Europe, G-Cloud (UK), Andromede (FR) and Trusted Cloud (DE) are leading examples.[17] In all these cases, the incentives cited are more efficient data centre utilisation as well as re-use of applications to standardise and keep costs lower. The UK quotes estimates of IT standard infrastructure utilisation of less than 10%.

A recent report has suggested that there are two ways to look at the adoption issues.[18] First, existing internal processes can be streamlined. Second, cloud can help to meet the increasing pressures to engage with citizens and businesses. Internal change requires: streamlining, migration while retaining reliability and service levels,updating and increasing the flexibility of legacy systems. Outward facing changes include adopting new delivery models that make sense to users of public services, e.g. services based on life events rather than the department that is delivering the service. This often requires connections between existing systems and multi-agency cooperation.

Table – Public sector benefits from cloud provisioning

Internal benefits	Outward looking benefits
Reduce capital and operating costs of existing systems	Shift to user-centric & joined up services
Better operational performance of technology and service	Active engagement of citizens and businesses
Better manageability	Reduced cost and complexity of service provision
More flexibility and agility	Lower cost of introducing new services
Lower upgrade costs	Pay for computational services on demand and at lower marginal rates

[17] US Government (2011) Cloud First http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf, HM Government (2011) Government Cloud Strategy, www.cabinetoffice.gov.uk, Ministère de l'Economie (2011) www.economie.gouv.fr/cloud-computing-investissements-d-avenir, BMWi (2010) www.trusted-cloud.de/documents/aktionsprogramm-cloud-computing.pdf

[18] Capgemini (2012) The Government Cloud: Time for Delivery, www.capgemini.com

Better cost control	Better monitoring and transparency of outcomes
Possibility of multi-agency/ shared platforms, reducing costs	

Source: adapted from Capgemini (2012)

Just as many of the gains and risks are similar, so the processes of adoption of cloud by public organisations follow the same pathways as for many large private adopters. As with private organisations, the tendency is to start cautiously with one relatively low risk application (i.e. one that is not mission critical and does not involve the treatment of sensitive data) or one that is inherently outward facing (such as consultation of citizens or for public relations). At the same time more sensitive or important data is kept on dedicated systems, either traditionally on-site or in outsourced data centres.

Certainly some of the benefits from cloud computing can be achieved through multi-agency use of private clouds as it permits consolidation of IT assets (data centres, networks and software) and further cost reduction through greater opportunities to construct and share common solutions and re-use of these solutions (both the US and UK governments have enthusiastically promoted the concept of government "app stores" for this purpose). The UK has also emphasised the need to move to new procurement models that are better adapted to operating expenditure rather than capital spending as befits the service nature of the cloud. This however creates problems in procurement as IT budgets are normally classified as capital expenditure. Issues of 'loss of control' are being tackled in the UK through attempts to define performance indicators and service assurance metrics, which would also apply to data security. The focus of the French strategy in contrast, has been to develop a sovereign (and therefore secure) infrastructures with an injection of 75m€ of public funds into an overall investment of 225m€. for the Andromede IaaS service to be set up by Orange and Thales. A further secure cloud computing joint venture between SFR and Bull will also receive 75m€ support from the French State National Digital Society Fund managed by the Caisse des Depots.

The UK plan sets targets for 50% of new central government spending on public cloud services by 2015, with cumulative savings of £340m. But, overall the public sector in Europe is cautious. Cloud usage so far is complementary to existing systems at best and thus not likely to yield the high cost savings that governments are seeking in their cloud strategies. Thus a strategic lead is needed not only at national level but also in each organisation.

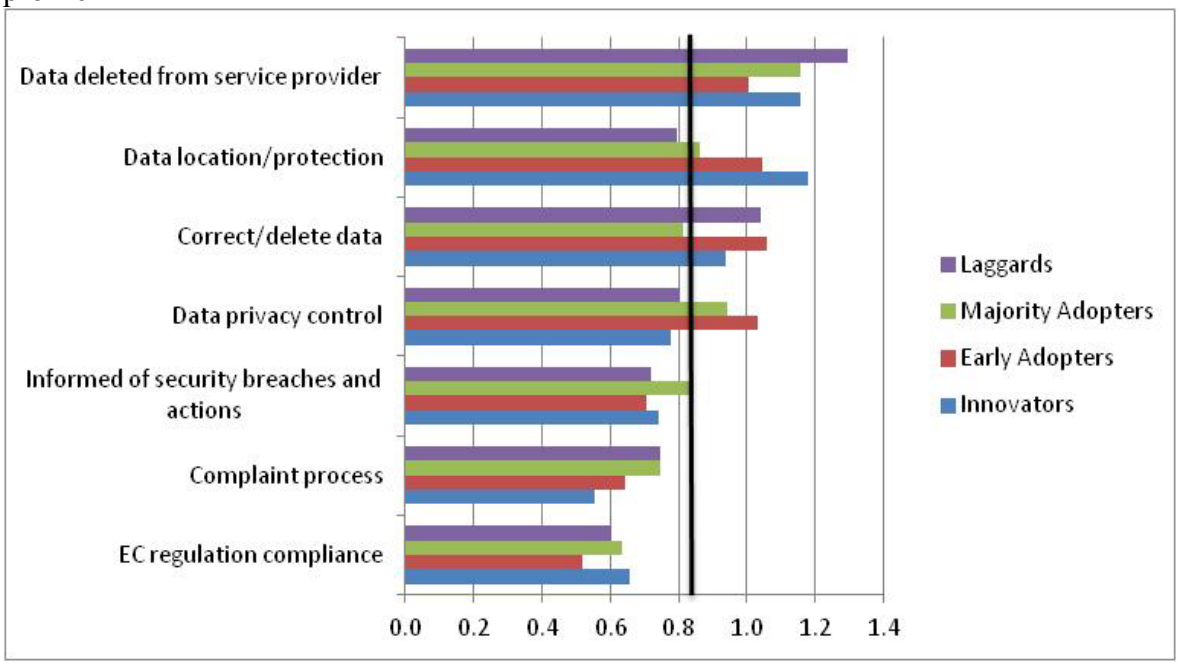
3.5. Cloud take up by consumers

IDC split consumers into four groups: innovators (who want to be amongst the first to try new things), early adopters (the next wave of adopters who read the reviews first), majority adopters (who want to see people they know using the technology first), and laggards (those who buy only when they have to).

While consumers do not generally recognise the term "cloud" for what they do online, a significant amount of what they do is what IDC would classify as consuming cloud services. One trend that emerged from the survey is that consumers will adopt services according to the utility that the service offers to them, and they will stop using these services when they stop

being of use. However, the laggards tend to hold back because they cannot see the usefulness of the service available to them, so they adopt a much narrower range of services.

FIGURE 3 The most important barriers to cloud adoption by consumer profile



Consumer adoption is mostly driven by the perceived utility of the services. Security and other "hygiene" factors such as data location / jurisdiction are less consciously important in their choices. When it comes to barriers to adoption however there are: an adequate complaint and compensation process in case of security breaches or data losses; due information and actions taken, when security and personal data breaches occur; the right to be forgotten (data does not remain in the service providers' archives); easy deletion of data; direct control over personal data through privacy-protection settings; transparency on data location and due diligence on the part of the provider as regards data location and protection; that the service complies with EC regulation on consumer protection, data and privacy protection (EU regulation compliance) (Figure 3).

Thus, whilst it does not seem to affect their online behaviour most consumers seem to expect that their rights and privacy online will be protected. This indicates a need for both increased self awareness on the reality of the risks of using cloud services as well efforts by service providers and public authorities to make sure appropriate measures are enforced to protect consumers in the cloud.

3.6. Conclusions on take-up

The main concerns about cloud services are security, data location, applicable law and jurisdiction over data, though on the last point it appears that most organisations surveyed lacked a full understanding of the complex issues. Data and application portability between cloud service providers does not appear to be a significant barrier to initial adoption, but becomes more important when the issue is deepening and extending the use of cloud in the enterprise. The top four actions that are important to most of the different adoption groups are:

- Greater accountability and liability for security by cloud services providers. At present, the majority of public cloud services providers tend to work on a "best efforts" basis, using their corporate reputation as evidence of the availability and security of their services. However, all the full users of cloud services and those who do not use the cloud see this as a factor that, if addressed, would increase their use of cloud. Limited users also see some potential benefit from changes in this area.

- Ensuring portability between cloud services. This is an important action for organisations that use cloud in more than one area, those that have some limited use of cloud services and (to a lesser extent) those that have full use of cloud services in one area. Portability does not seem to be a barrier to using cloud services in the first instance – after all, portability between on premise systems is generally poor. However, it becomes an issue when organisations are already using cloud services.

- Improving broadband connections is important to initial adoption as it is cited as a constraint by non-users of the cloud overall and also to limited users. Full users of the cloud can be assumed to already have good connectivity as it is a pre-requisite for the adoption of cloud.

- Security certification of cloud services vendors did not score particularly highly for any one group but overall it is fourth in the ranking across all the responses to the survey.

In a multi-dimensional analysis of the impact of the different barriers to adoption it was found that jurisdiction issues, security and trust, data access and portability will remain high importance for all categories of adopter over the longer term (Table 1).

TABLE 1: The relevance of barriers to adoption over the long term

Cluster	Barrier	Long -term relevance of Barrier	Relevance for large companies	Relevance for SME Companies	Relevance for the Public Sector	Relevance for the Private Sector
Data jurisdiction and location	Legal Jurisdiction	High	High	High	High	High
	Data location	High	High	High	High	High
Security and Trust	Security& data protection	High	High	High	High	High
	Trust	High	High	High	High	High
Portability and technology transparency	Data Access and Portability	High	High	High	High	High
	Ownership of customisation	Medium	Medium	Low to medium	Low to medium	Low to medium
	Change control	Low	Low to medium	Low	Low to Medium	Low
Business	Evaluation of Usefulness	Medium	Low to medium	High	Low to medium	Medium
	Local support	Low to medium	Low	Low to medium	Low to medium	Low
	Local language	Low	Low	Low	Low	Low
Industrial policy	Tax incentives on capital spending	Medium	Low to medium	Low	Medium	Low to medium
	Slow Internet	Medium	Low to medium	Medium	Low to medium	Low to medium

	Connection					

Table x2compares the industry recommendations presented to the European Commission in December 2011 with the relevant findings from this study. As the table shows, there is evidence that this survey supports these recommendations. These findings are also heavily corroborated by a recently published report funded by the European Parliament's Economic Policy Department, which identifies key barriers to the digital single market in cloud computing as:[19]

- Fragmentation of the digital single market due to differing national or regional legal frameworks: the report considers that fragmentation is due to a limited level of harmonisation in the digital content and electronic communications. Rights and responsibilities in the cloud not yet being clear due to lack of transparency or difficulties in finding information, problems with contracts, the complexities of multiple jurisdictions or the fact that for different legal issues - data protection, contracts, consumer protection or criminal law - the jurisdiction may differ.

- Cloud provider contracts which disclaim liability, might contain unfair or illegal clauses and lack certain key pieces of information such as the location of data centres. In particular, service contracts offered to SMEs are rigid, with little room for negotiation. Stakeholders called for standardised contracts, with specific requirements regarding safety, security and reliability.

Standardisation efforts for cloud services are proliferating, whereas support for interoperable standards from industry is mixed, with some industry players fearing that early standardisation could stifle innovation. Table 2: Recommendations from Industry compared to findings of IDC study

Industry Recommendations	**Findings of the Study**
Clarifying and harmonizing the legal framework for cloud	This is very much supported from this study. This issue is the key issue for all stakeholders and also ranks high from our enterprise study with respect to
Raise awareness and encourage uptake of cloud	This comes out as an action from the stakeholders – with much the same flavours as the Industry's detailed recommendations (public sector lead by example, information sharing, portals)
Proper response to data breaches	Although this does not **directly** come out strongly in this study, **implicitly** it does as issues such as security, vendor liability, SLAs and auditability are important. Security is the largest concern amongst enterprises about cloud.
Certification (industry-led)	A framework for certification is amongst the most important actions for the EU to take. The stakeholder interviews show that mostly vendors think the industry should drive this
Foster and fund research	This is an issue that is also brought up in the stakeholder interviews, particularly from

[19] European Parliament (2012) Cloud Computing Study for Policy Department, economic and scientific policy, http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=73411

	experts and vendors.
Foster interoperability and data portability	This study confirms this to be the top issue amongst enterprises and it is also one of the key actions from stakeholders. In the enterprise survey, this issue does not appear to block adoption of cloud services, but it does become a key concern once enterprises have adopted the cloud.

In conclusion, stakeholders believe that the main actions that the EU should take concern clarification of the applicable law and jurisdiction, where relevant, harmonisation of the national legal frameworks – and to some degree – standardisation and certification of cloud and cloud services. These top barriers are however highly correlated indicating that there is a cumulative negative impact on cloud adoption. Moreover if these barriers were to be removed

- More than 98% of EU companies would start or strengthen investments in cloud solutions.
- The cloud would attract new users: 94% of companies that are currently thinking about cloud adoption (but without formal plans yet) would start investing. 94% of companies that are currently not even thinking about cloud would also start investing.
- Cloud intensity will strengthen across the board. On average, EU companies would move up to four cloud solutions (as compared to today where only 32% of firms are using cloud in more than one area).

In the case that these barriers are resolved, the "policy driven" scenario in the study indicates that

- Public cloud spending would grow at a 38.3% compound annual growth rate reaching to nearly €80 billion in 2020 against €35 billion in the "no intervention" scenario.
- Growth rates would strengthen across all vertical markets, and in particular in the government sector.
- SMEs (especially companies with 100-249 employees) would increasingly rely on cloud solutions and their share of total public cloud spending would increase to 25% in 2020. In particular, cloud would help EU SMEs gaining efficiency and help their competitive position on the global market.
- Moreover, IDC estimates that the public cloud would generate some €250 billion GDP in 2020 in the policy driven scenario against €88 billion in the no intervention scenario, leading to extra cumulative impacts of €600billion as against the "business as usual" scenario.

4. SUMMARY OF CONSULTATION RESULTS

This section reports on the main results of consultation undertaken during the development of the cloud computing strategy.[20]

[20] All reports are published at: http://ec.europa.eu/information_society/activities/cloudcomputing/library/index_en.htm

(a) A public web-based consultation opened on 16 May 2011 and closed on 31 August 2011. The main conclusions were:

(b) The EU **legal framework** within which Cloud Computing must be implemented is sometimes not well known. Participants asked for clarification on rights, responsibilities, data protection and liability, especially in cross-border situations. Guidelines on good practice in contracting, model contract terms and conditions, reasonable expectations for service level agreements would be appreciated. The **public sector**, as cloud computing adopters, could set the requirements for standards in security, interoperability and data portability;, stimulating more rapid cloud deployment. Resolution of the single digital market issues is only a partial solution since Cloud Computing is inherently embedded in a global infrastructure. **International agreements are seen as necessary** in key areas such as certification, data protection and security. Finally, current Cloud Computing technology can be improved through **research and development**, notably integration of other distributed computing models.

(c) A select group of high level industrial representatives were consulted in a process starting in May 2011. The group presented legal, market and technical recommendations to VP Kroes in December 2011, covering data privacy, trust and security, interoperability and portability and stimulating take-up.[21] Barriers identified to take up were security (uncertainty on compliance), reliability and availability for business critical tasks, data privacy and integrity, lock-in, transfers of legal liability, network performance and general lack of know-how or awareness on getting business benefits. From the vendors perspective the problems are the costs of managing requirements to keep data located inside the relevant jurisdictions and adapting business models.

(d) The group identified three areas of recommendations. 1) Legal frameworks should be harmonised globally or at least at the level of the single market and existing rules should be checked for their compatibility with the cloud. 2) The Commission was called upon to promote the take-up of cloud by SMEs and the public sector, supported by industry, for example by building use case scenarios. There should be a platform for further discussion between all stakeholders where issues such as transparency and security could be addressed. The group called for voluntary certification mechanisms to enhance trust and security. 3) A strategic research agenda should be developed and pilot projects supported. The group called for a comprehensive inventory of existing cloud standardisation and interoperability initiatives. A roadmap towards data portability was seen as a task for industry to ease migration to cloud systems.

(e) Further focussed discussions were held with specific stakeholder groups:

- SMEs were invited to a consultation on 14 November 2011

[21] See Industry Recommendations To Vice President Neelie Kroes On The Orientation Of A European Cloud Computing Strategy; http://ec.europa.eu/information_society/activities/cloudcomputing/docs/industryrecommendations-ccstrategy-nov2011.pdf

Given the diversity of SMEs and the broad range of issues to be addressed, SMEs' key requirement is **their need for objective and understandable information about the cloud**, from neutral channels, so as to be able to assess the costs and benefits and make a balanced choice. In particular, SMEs see a need for a new mindset in order to make the step towards cloud computing.

- Telecommunication providers were invited on 16 November 2011 They:

    - regard cloud computing as **essentially** an **information society service**, rather than a telecoms service. Cloud services can be delivered either on a standalone internet basis (with no link to access components), or in a bundle with a dedicated access service, or through subscription to an Internet Service Provider. In each case, they argued that cloud computing is **distinctively an information society service** which falls outside of the telecoms remit.

    - are concerned however that the current e-communications framework subjects them to numerous obligations in relation to data protection and privacy that do not apply to IT providers. Location data collected by telecoms providers are regulated whereas there are no similar provisions for such data collected by other service providers. Telcos are also subject to stringent provisions on data retention which do not apply to other providers.

    - regard the liability exemptions in the eCommerce Directive as well balanced and that no major revisions were necessary. However, according to them, , the obligations of 'notice and action' provisions for illegal content should be clarified.

    - see enterprises liability provisions a subject for through contract negotiation. However model contract terms and conditions and voluntary best practice guidelines would increase awareness and compliance.

- Large user organisations

The European CIO organisation submitted separate recommendations to VP Kroes in January 2012[22] in response to a consultation of large user organisations on 21 November 2011.

> In general this group sees the cloud as offering huge economic potential for Europe, especially for large users of IT. Usage-based pricing, reduced total cost of ownership and no upfront capital investment are key benefits, while companies will be able to move more quickly and reduce their time to market.
>
> Security of data was cited as the main barrier to cloud computing adoption. Trust in putting data in cloud-like resources is often lacking. The cloud brings important security challenges. Participants outlined an extensive list of measures they would like to see taken, such as:

[22] The CIO report is published here: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/consolidated_list_of_recommendations_users_%20perspective.pdf[1].pdf

- Greater transparency in data security governance
- Standardized terms of service
- Minimum retention of data
- Shared data as a legal concept
- Jurisdiction and Data Protection
- Interoperability and Standards

- Consumer representatives

The consumer organisation, BEUC, was invited to a consultation on 22 February 2012. BEUC sees many benefits from Cloud Computing for the user: such as the possibility for larger storage capacity (e.g. for photo sharing websites), convenience and ubiquitous access (e.g. webmail), reduction of expenditures leading to lower cost and tax (e.g. use in companies, e-health and governments) and the possibility of innovation.

> Their main concerns are the adequate protection of personal data, consumer protection, and interoperability especially in connection with data portability. They see these issues as needing action to ensure further consumer uptake of Cloud Computing.

5. CLOUD COMPUTING AND DIGITAL AGENDA (DIGITAL SINGLE MARKET)

5.1. Digital Agenda Actions – "opening –up access to content"

There is considerable consumer demand for cloud-based content distribution models allowing content access and content exchange from different devices and different territories.

In this context, for cloud computing services, questions arise in particular with regard to (1) the possible collection of private copy levies for copying content in the cloud, (2) the possibility for the upload and/or storage in the cloud, (3) the possibility to access this content from the cloud and/or to make private copies of it.

5.1.1. Private copying regime in the cloud environment

In many Member States which have introduced the private copying exception[23], private copying levies are imposed on certain categories of media (such as recordable CDs or DVDs) and devices (such as MP3 players) which are typically used for private copying. When introduced in the analogue age, the private copying levies system was seen as a sensible recognition that not all acts of reproduction can be licensed and that rights holders should be compensated for the harm resulting from non- licensed copies of protected content, made by natural persons for their private use. Private copying levies were first introduced for analogue equipment and media and charged on single-function devices designed and intended to be used for private copying.

[23] Art. 5(2)(b) of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

5.1.1.1. The current private copying levies system

Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society[24] ("Information Society Directive") permits Member States to provide for an exception to the exclusive right of reproduction in respect of acts of private copying. In such a case, rightholders must receive a "fair compensation"[25]. The Information Society Directive does not state the means for calculating fair compensation in detail. As there is no European harmonization of private copying levies, there are considerable differences between countries in that regard.[26]

The lack of harmonisation (which has distortional effects on the single market in the EU), legal uncertainty and the absence of synergy between traditional levy systems and the new technical digital environment all could cause serious economic problems for the ICT and entertainment hardware industry in Europe, as well as for right holders in the absence of any rules on jurisdiction and applicable law for cloud computing. Differences between national private copying levies systems have been identified as one of the obstacles to cross-border e-commerce and a major barrier to the establishment of a Digital Single Market in the strategic report to President Barroso carried out by Professor Mario Monti[27].

5.1.1.2. Mediation on private copying levies

The European Commission adopted on 24 May 2011 a proposal for a Communication "A Single Market for Intellectual Property Rights"[28] in which it announced the appointment of an independent mediator on private copying and reprography levies.[29]. In April 2012, Mr. António Vitorino, on whom this task was conferred, has started a process of mediation which brings key stakeholders together in order to identify key elements on which a workable agreement could be found. It touches in particular upon issues such as the devices subject to a

---

24 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

25 Article 5(2)(b) reads: "Member States may provide for exceptions or limitations to the reproduction right] "in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly or indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures [referred to in Article 6."

26 At present, most Member States provide for a private copying exception (excluding Cyprus, United Kingdom and Ireland) and provide for fair compensation by levying certain goods that are typically used for the production of a private copy (blank media, recording equipment, mobile listening devices, computers, printers, scanners, etc.). Luxembourg and Malta provide for a private copying exception but have not introduced a system of fair compensation. The UK, however, has recently announced its intention to introduce a limited private copying exception without a corresponding copyright levy regime. In the 22 Member States in which copyright levies have been introduced, the scope of the exceptions, the level of the levies and the products to which levies apply all vary materially from Member State to Member State. The application and the amount of levies are disputed and are increasingly being challenged in courts in Member States, especially with regard to modern ICT and digital entertainment hardware and storage media.

27 Professor Mario Monti, Report on on a new strategy for the Single Market, 9 of May 2010.

28 Communication *A Single Market for Intellectual Property Rights: Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe*, Communication from the European Commission (COM(2011) 287 final)

29 Section 3.3.4 of the Communication "*A Single Market for Intellectual Property Rights"* reads: "The proper functioning of the internal market also requires conciliation of private copying levies with the free movements of goods to enable the smooth cross-border trade in goods that are subject to private copying levies. Efforts will be redoubled to kick-start a stakeholder agreement built on the achievements of a draft Memorandum of Understanding (MoU) brokered by the Commission in 2009."

levy, the methodology for tariff-setting and cross-border sales. At the same time, private copying – its scope, its justification- is being analysed in the context of new digital forms of distribution of copyright- protected content and the development of new business models. [30]

On the basis of the results of this mediation process, the mediator will formulate recommendations on which the Commission will base a decision on appropriate follow-up steps.

5.1.1.3. Cloud computing services challenges to the private copying levies regime

In the context of private copying levies it is important to take into account the development of new technologies, in particular cloud computing services.

Some of the technologies applied in the digital context, such as streaming, have the potential of reducing the number of copies which are actually made on consumer devices. Cloud computing services, where end-users are actually replicating less on their personal local devices have been seen as a game changer, making the private copy levy concept less appropriate, as digital technology advances[31]

Increasingly, cloud based services make it possible to measure authorised uses of creative content allowing for a precise licence-based remuneration (and not exception-based compensation) of right owners. This should clearly be the case where a specific cloud-based service has been established following a licensing agreement with rightholders. Furthermore, streaming of music (or audiovisual content) does not require consumer storage capacity – i.e. music or audiovisual files are not necessarily downloaded onto the device's memory. In such cases, applying levies on the basis of memory size does therefore not seem to be aligned with the way music or audiovisual content are consumed.

According to the ECJ, fair compensation must be calculated on the basis of the criterion of the harm caused to authors of protected works by the introduction of the private copying exception.[32] Still, where the equipment at issue has been made available to natural persons for private purposes, it is unnecessary to show that they have in fact made private copies with the help of that equipment and have therefore actually caused harm to the author of the protected work. It follows that the fact that the equipment is able to make copies is sufficient in itself to justify the application of the private copying levy, provided that the equipment or devices have been made available to natural persons as private users.[33]

Currently, depending on the national private copy levy system, private copy levies are being asked for the storage media and the hard ware used by consumers in the context of cloud services.

With the emergence of new business models, consumer-friendly access to attractive legal offers of digital content should be more focused on licensing than on private copying levies. The more digital content and authorised usage consumers are able to acquire as part of a fully licensed service, the less need there is for private copy levies by way of compensation. This has been indicated in the Kretschmer Report[34], which states that "Since private copying can

30 http://ec.europa.eu/commission_2010-2014/barnier/docs/speeches/20120402/statement_en.pdf

31 See, M. Kretschmer, "Private Copying and Fair Compensation: An empirical study of copyright levies in Europe**",** A Report for the UK Intellectual Property Office, October 2011.

32 European Court of Justice, Judgment of 21 October 2010, Padawan, C-467/08 at 50

33 European Court of Justice, Judgment of 21 October 2010, Padawan, C-467/08 at 54, 56

34 See, M. Kretschmer, "Private Copying and Fair Compensation: An empirical study of copyright levies in Europe**",** A Report for the UK Intellectual Property Office, October 2011.

be permitted under contract, there is no need for an exception. The appropriate compensation is a licence fee which should be left to the market."[35]

In addition, the Hargreaves Report "Digital Opportunity" indicated that a number of "cloud-based services" are used as a mere backup or to transfer content to other devices which are themselves already covered by the private copy regime. It is argued that copies reflecting standard consumer behaviour are already factored into the prices of retailers, therefore resulting in no actual harm to the author.[36]

Fair and efficient transactions between rightholders and cloud services providers as well as between cloud service providers and consumers should allow equitable and efficient remuneration of rightholders. It is essential to take proper account of the opportunities offered by the current development of new business models. Such models deliver new forms of authorised access to copyright protected content. They should at the same time enable rightholders to better control the use of their content and the manner in which they are remunerated for it.

5.1.2. Flexible copyright licences for cloud services

The Communication "A Single Market for Intellectual Property Rights" states that the creation of a European framework for online copyright licensing would greatly stimulate the legal offer of protected cultural goods and services across the EU. Modern licensing technology could help make a wider range of online services available cross-border or even create services that are available all over Europe[37].

5.1.2.1. Efficient and transparent mechanisms for rights clearance and the data management features of cloud computing;

As regards Cloud Computing based services, as with all on line services, there is a need to find solutions to make copyright licensing more efficient. Hence, the rights clearance processes should be efficient and transparent, particularly with regard to collective rights management. Making such licences easy to acquire could drive innovation and create new revenue streams for rights holders. The recent legislative proposal put forward by the Commission[38] will improve the functioning of collective management across the board and ease the licensing of authors' rights for the use of music on the Internet. This should lead to improved access to and more offer of, inter alia, music online.

Moreover, the Commission already announced it will encourage and support projects undertaken by various stakeholders to develop automated and integrated standards-based rights management infrastructures.

---

35 See, M. Kretschmer, "Private Copying and Fair Compensation: An empirical study of copyright levies in Europe**",** A Report for the UK Intellectual Property Office, October 2011, p. 58

36 In the current debate in the UK it is argued that "[a] limited private copying exception which corresponds to the expectations of buyers and sellers of copyright content, and is therefore already priced into the purchase, will by definition not entail a loss for right holders." (Hargreaves Report, "Digital Opportunity", p. 49: http://www.ipo.gov.uk/ipreview-finalreport.pdf). The UK Government agrees with this assessment (See: UK Government Response to the Digital Opportunity Report, pp. 7-8 http://www.ipo.gov.uk/ipresponse-full.pdf), also relying on the findings of Professor Martin Kretschmer's Report (See: M. Kretschmer, "Private Copying and Fair Compensation: An empirical study of copyright levies in Europe**",** A Report for the UK Intellectual Property Office, October 2011.)

37 Communication "A Single Market for Intellectual Property Rights" COM(2011) 287 final, p.10

38 Proposal for a Directive of the European Parliament and of the Council on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online uses in the internal market, COM(2012) 372 final.

The ongoing industry-led projects focus on quality of information available to different actors in the copyright licensing chains and its efficient flow. They include the Linked Content Coalition[39] the objective of which is to develop a standards-based communications infrastructure to enable the more effective management of copyright online and the Global Repertoire Database[40] project aiming at providing, for the first time, a single, comprehensive and authoritative representation of the global ownership and control of musical works.

In parallel, the idea of a Digital Copyright Exchange (DCE) is being explored in the UK: following up on the Hargreaves Report, the UK Government has appointed Mr Richard Hooper to lead a DCE feasibility study. If successful, this initiative could stretch beyond facilitating information exchange between copyright licensing actors and result in an online platform connecting copyright owners or managers and users of copyright protected works.

5.1.2.2. Access to content in the cloud

Consumers and businesses could benefit from the economies of scale offered by the single market if cross-border barriers to e-commerce were removed. The use of new data storage media such as cloud computing could increase productivity in the audiovisual and other sectors even further. Cloud computing is more scale efficient at cross-border level and the technology is increasingly global in nature.

The Communication "A Single Market for Intellectual Property Rights" underlines that Europe must develop copyright licensing services, combined with web applications and tools, to foster vibrant cultural and creative industries that allow millions of citizens to use and share published knowledge and entertainment easily and legally across the Union irrespective of their Member State of residence.[41]

Moreover, The Commission announced in the above mentioned Communication that it will support measures to make it simpler and efficient to access copyright protected works through innovative licensing technologies, certification of licensing infrastructures, identification and data exchange of actual usage and electronic data management.[42]

Accessibility is the main advantage of cloud computing services for digital content. Providers of cloud based services can offer their customers the possibility of accessing content, no matter whether it is music, audiovisual or books, from different devices. This way, customers do not lose access to their library only due to the fact that they are using various devices or because they are on a business trip or holidays in another MS.

Service providers should be able to negotiate with rightholders, licencing agreements for such services, so that their customers are able, lawfully, to consume content away from home across the European Union. Cross-border licensing agreements should be supported to enable these kinds of services and thus create new revenue streams for rights holders.

The current copyright framework is sufficient to accommodate multiterritorial licencing. However, innovative and flexible approaches to licensing copyright protected works for cloud services need to continue to be developed and there is a need to assess how to incentivize rights holders to make their content available on a multi-territory basis, and cloud service providers to deliver their services on multi territory basis and how to enable consumers to access services from different Member States.

---

39 http://www.linkedcontentcoalition.org/Home_Page.html

40 http://www.globalrepertoiredatabase.com

41 Communication "A Single Market for Intellectual Property Rights" COM(2011) 287 final, p. 9 – 10.

42 Communication "A Single Market for Intellectual Property Rights" COM(2011) 287 final, p. 11.

The recent ECJ judgment in the Premier League[43] case has clearly established, as an important principle, while rights holders may license their property on a territorial basis, a restriction on the free movement of services cannot be justified in those cases where rights holders can achieve an appropriate remuneration without the need to impose territorial exclusivity. This judgment, even though it is limited to sports rights which are not protected by EU copyright law, could alter the way in which other types of content are licensed in the single market, most particularly content licensed using the model of the Satellite and Cable Directive, thus responding to increasing consumer demand. The forthcoming report on the consultation launched by the Green Paper on the Online Distribution of Audiovisual Works (the "*Audiovisual Green Paper*")[44] will examine, *inter alia,* how best to build on the judgment to the benefit of the Single Market.

The Commission will address issues relating to the country of origin principle in its forthcoming report on the outcome of the consultation launched by the Green Paper.

5.2. Digital Agenda Actions to "Make Online and Cross-Border Transactions Straightforward"

Information society service providers generally have a limited degree of knowledge about the content they transmit or store. The E-Commerce Directive[45] introduced, in Articles 12-14, a set of liability exemptions for activities provided by online intermediaries[46].

Articles 12-14 of the E-commerce Directive provide for a so called "safe harbour", in which three types of activities provided by online intermediaries are under certain conditions exempted from liability for illegal content. The three activities concerned are:

- "mere conduit" services, which comprise network access services or network transmission services (e.g. service provided by internet service providers).

- "caching" services, which comprise temporary and automatic storage of data in order to make the onward transmission of this information more efficient (e.g. service provide by web-sites). Caching is normally regarded as a technical process used to improve customer experience.

- "hosting" services, which comprise storage of data provided by their users. The data being stored is specifically selected and uploaded by a user of the service, and is intended to be stored ("hosted") for an unlimited period of time.

Furthermore, a service provider can conduct various activities of which some are intermediary (in the sense that the service provider transmits or hosts information from a third party) while others are not. The liability exemptions are only limited to the first category. They do not extend to all other activities carried out by a service provider (see specifically recitals 42 to 46 of the E-Commerce Directive).

---

43 ECJ Judgment ruled on 4 of October 2011, in Cases C-403/08 and C-429/08, Football Association Premier League and Others v QC Leisure and Others

44 COM 2011 (427), 13 July 2011. http://ec.europa.eu/internal_market/consultations/2011/audiovisual_en.htm

45 Directive 2000/31/EC (Ecommerce Directive)

46 .Information society services as provided for in Article 2 of Directive 98/34/EC as amended by Directive 98/48/EC.

The recently adopted E-Commerce Communication[47] concludes that although the E-Commerce Directive aims to be technologically neutral, innovations and economic developments since its adoption in 2000 have rendered the interpretation of above-mentioned provisions increasingly challenging and that it is thus necessary (among other things) to provide clarification concerning the liability of information society services providers, and take the additional measures needed to achieve the Directive's full potential, as identified in the current action plan. The Communication further underlines that despite the guarantees offered by the Directive on electronic commerce to businesses which host or passively transmit illegal content, intermediary internet service providers struggle with the legal uncertainty linked to fragmentation within the European Union of the applicable rules and practices which are possible, required or expected of them when they are aware of illegal content on their websites.
During the consultation preceding the Communication, stakeholders pointed out divergent national case law that has emerged particularly with regard to the application of liability exemptions to "new services" that are not explicitly mentioned in the E-commerce Directive as location tool, hyperlinking or cloud services. This has resulted for them in a degree of regulatory uncertainty." [48]
One example of this uncertainty can be given with a case law on "Usenet", which has been qualified by the German Regional Court of Munich as a caching provider and by other courts as a hosting service[49]. In another case, the Italian Court of Cassation[50] considered that PirateBay was not a hosting service provider. However, the Stockholm District Court[51] found that Pirate Bay provided a service where a user could upload and store torrent files on the website, and the service was, consequently, deemed to be a ‘‘hosting’’ service.

5.3. Digital Agenda Actions on Building Digital Confidence

International rules allowing unchecked and extraterritorial access of law enforcement authorities and security services of certain countries to EU data stored in the cloud by providers from outside the EU are among the biggest obstacles to cloud uptake by business users in Europe. In this context, the question whether and how EU data protection law applies is essential.

Some concerns were also raised by cloud computing stakeholders mainly as to the scope of the current EU date protection legal framework and to the respective obligations of data controllers and data processors. Some of these interrogations were also conveyed by the Article 29 Working Party. This has shown the necessity to introduce an even more clear and integrated legal framework at EU level.

---

47 Communication on "A coherent framework for building trust in the Digital Single Market for e-commerce and online services", COM(2011) 942 final

48 For more details, see the Staff working document "Online services, including e-commerce, in the Single Market", chapter 3.4.2 in particular.

49 LG Düsseldorf, 23 May 2007, 12 O 151/07, MMR 2007, 534 (535); Queen's Bench Division, 10 March 2006, *Bunt v. Tilley,* as mentioned in T. VERBIEST, G. SPINDLER, G.M. RICCIO, A. VAN DER PERRE, *Study on liability of Internet intermediaries*, ordered by the European Commission, November 2007, p. 34

50 Cour d'Appel de Paris, 08/09553, 21 Novembre 2008,

51 Court of Cassation, Third Criminal Chamber, 49437, 29 September 2009

5.3.1. Stakeholders'concerns

(a) In the consultation process and in the background studies undertaken in preparing the cloud computing Communication as well as the European Parliament cloud computing study[52],[53] cloud computing was cited as one of the factors driving the reform, with the aim of producing a robust and coherent EU regulatory regime that would ensure the effectiveness of data protection and engender trust for cloud services providers[54].

(b) Moreover, the 2011 report "The Cloud Understanding the Security, Privacy and Trust Challenges", undertaken for the European Commission, presents an overview of gaps in various aspects of current European policy approaches relevant to cloud computing. It identifies, as regards the Data Protection Directive, the following legal gaps: "1.1 The definition of data controller/processor and applicability of these terms on cloud models; 1.2 Control over personal data; 1.3 Location as a criterion for determining applicable law, in combination with differences between national laws; 1.4 Rules to support accountability may not be effective or optimal"[55]The Industry Recommendation on the orientation of a European Cloud computing strategy[56] states that in the cloud computing context the division between controller and processor will become more complex. Controller, processors, sub-processors and allocation of functions across a continuum of roles makes some existing definitions in the Data Protection Directive less relevant or applicable.The same Industry Recommendation further underlines "the lack of clarity on applicable law, especially in cross-border situations where the data subject, the data, the controller, the processor and the processing are located in different countries, within or beyond the EEA". There has also been a lack of certainty about applicable law. The place of establishment of a cloud service provider may be hard to determine, e.g. for a non-EU user of a non-EU provider operating a data centre in Europe. The Commission has recently proposed a Data Protection Regulation as a single set of rules at EU level and a "one stop shop for enforcement" in one of the most important areas touched by cloud.[57]The proposed Regulation constitutes a good general basis for the future development of cloud computing, The Commission will work with Council and Parliament towards the adoption of the proposed Regulation in 2013. Under the current data protection

---

52 See: Study on Cloud Computing, Civic Consulting, prepared for the European Parliament, Dg Internal Policies of the Union, June 2012 http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=73411.

53 See: Study "Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up", D3 – Analysis of the demand of cloud computing services in Europe and barriers to uptake, IDC (2012) op. cit.

54 European Commission, 'Data protection reform: Frequently asked questions' (25 January 20121) MEMO/12/41. The draft Regulation is 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM(2012) 11 final 2012/0011 (COD).

55 See: The Report "The Cloud Understanding the Security, Privacy and Trust Challenges" prepared by the RAND Corporation for the Commission, DG Infso, 2011 available at http://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR933.pdf

56 See: Industry Recommendations on the Orientation of a European Cloud Computing Strategy, November 2011avilable at: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/annex-industryrecommendations-ccstrategy-nov2011.pdf

57 A European Data Protection Framework for the 21st Century, COM/2012/09

directive 95/46/CE, the Commission will in addition work on specific measures to ensure that data protection rules can be applied to cloud computing in an effective manner.In the meantime, the Article 29 Working Party, has recently outlined how "the wide scale deployment of cloud computing services can trigger a number of data protection risks, mainly a lack of control over personal data as well as insufficient information with regard to how, where and by whom the data is being processed/sub-processed". This Opinion examines issues associated with "the sharing of resources with other parties, the lack of transparency of an outsourcing chain consisting of multiple processors and subcontractors, the unavailability of a common global data portability framework and uncertainty with regard to the admissibility of the transfer of personal data to cloud providers established outside of the EEA".This Article 29 opinion clarifies the expectations of data protection authorities for controllers and processors in the context of cloud computing. It stresses that it is important that cloud customer are properly informed. It states also that in the contracts it should be specified their expectations in terms of protection of personal data to cloud providers in order to ensure the effective protection of the personal data under their control.

(c) The concerns raised by cloud users and providers mainly focus on the scope of the EU data protection Directive, most of them in relation with the criteria of the equipment and, to some extent, with the notion of "processing (…) in the context of the activities of an establishment of the controller".

More generally, the main issue raised by cloud computing stakeholders is that under the current framework, cloud providers might sometimes have to comply with several national laws. It was noted that, on the one hand, it can lead to excessive burden for the providers or, on the other hand, to jurisdiction shopping if some jurisdictions require more stringent data protection safeguards than others.

5.3.2. The proposed data protection Regulation

The concerns of cloud operators and users were carefully considered during the preparatory work for the Data Protection Regulation recently proposed by the Commission.

On this basis, the Regulation provides for a single set of rules at EU level and "one stop shop enforcement"[58]. This means that only one Regulation will apply within the Union, independently form the place of establishment of the cloud service provider.

The proposed Regulation constitutes a good general basis for the future development of cloud computing.

As to the respective obligations of data controllers and processors, the proposed leaves it to operators to agree on the detailed rules of their relationship and respective responsibilities themselves. The complex service provision involving chains of providers and other actors such as infrastructure or communication providers can thus be organize with tailor made solutions within a stable system of a regulation ensuring that only one comprehensive law is applicable across the EU.

The proposed Regulation facilitates transfers of personal data to countries outside the EU and EEA while ensuring the continuity of protection of the concerned individuals. The Commission will have the power to recognize the adequate protection offered not only by a

[58] A European Data Protection Framework for the 21st Century, COM/2012/09.

third country but also by an economical sector. The new legal framework will provide for the necessary conditions for the adoption of codes of conduct and standards for the cloud, where stakeholders see a need for certification schemes that verify that the provider has implemented the appropriate IT security standards and safeguards for data transfers.

5.4. Cutting through the Jungle of Standards

In the ICT sector, it is common that existing products are used as building blocks for new products or systems. These additions quite often enhance the value of the original products and lead to innovation for users.

In order for this development and innovation to happen, innovators need to have information about interoperability information for the devices and applications with which they want their products to be compatible. This interoperability information can be made available by the owners of these devices and applications, if they decide to do so. A standardisation process is often the vehicle for this. Interoperability is also critical for users to be able to use multiple cloud providers. If this is achieved the end result will be a more competitive market that is better able to serve consumers. In the field of cloud computing there is at the moment no common agreement as to which standards would guarantee the needed interoperability. A common standard would need to be established.

In general, each vendor has an incentive to achieve dominance through lock-in which inhibits interest in standardised, industry-wide approaches. Thus despite numerous attempts to develop standards for clouds, mostly led by suppliers, there is a strong risk that clouds will **lack interoperability and data portability** (withdrawal of data**)**. The latter is crucial feature for competition as a distributed data environment cannot be easily moved to another platform. It will also help to open the market and avoid that a supplier could be tempted to abuse a dominant position.

User are not in a position to evaluate suppliers' claims as to their implementation of standards, the interoperability of their clouds or the ease with which data can be moved from one provider to another. For this purpose, independent, trusted certification is needed.

In this context, the Data Protection Directive requires data controllers and processors to apply technical and organizational measures defined in their contracts and compliant with the law to protect data against accidental or unlawful destruction, loss, disclosure, and other forms of unlawful processing. The proposed Data Protection Regulation foresees the introduction of the principle of data protection by design and by default, the introduction of data breach notifications and the introduction of privacy impact assessment and reinforces the obligation of processors

Moreover, information security is probably the biggest concern for companies when considering cloud adoption. Cloud service users need to be confident that their services and data are secure in the cloud. The data need to be always available to them and not accessible to unauthorized users. Cloud specific security risks relate to the multi tenancy and shared resources character of cloud computing. They are related for example to access control, data storage, data protection, data portability, data integrity and virtualisation. In the cloud the client cedes control of the security to the service provider thus making it more difficult to assess whether the cloud service provider (CSP) can comply with the security requirements in sufficient way.

As the (CSP) takes over the whole responsibility for security from the client there is a heightened need to ensure the transparency of the CSP's security practices towards the client. Also of concern is the interoperability of clouds which is closely related to data formats. At the moment cloud computing lacks security standards and international certification schemes, which would help to harmonise practices across cloud providers and which would make the clients more aware of what they should expect from CSP.

Although the security risks in the cloud do not necessarily differ technically from the risks known already (such as DNS or DoS attacks) the risks can amplify quickly and easily in the cloud which increases the effects on multiple clients simultaneously. According to an ENISA study on security in the cloud the top cloud-specific risks are[59]:

Loss of governance; in using cloud infrastructures, the client necessarily cedes control to the Cloud Service Provider on a number of issues which may affect security. In theory the service level agreements should cover the security measures put in place by the CSP. In practice, the client has very little information and influence on the security management of the cloud providers.

Lock-ins: The data formats and service interfaces in the cloud are not standardised. Therefore the clients do not have any guarantees of continuity of the service when changing to another CSP or when migrating data and services back to an in-house IT environment

Isolation failure: In a multitenant environment the failure of mechanisms separating the storage, memory and routing between tenants is a risk. Attackers can make use of vulnerabilities in these mechanisms to reach the domain of a tenant by entering the domain of a co-tenant of the same cloud. Minor miss-configurations can endanger large amounts of data.

Reputation: Damage due to security malpracticee of a CSP to the reputation of one tenant in the cloud could also sffect the reputation of other tenants in the cloud.

Virtualisation: Cloud service provision in often based on virtualisation, meaning that the real operating platform system of the CSP is hidden from the clients. There are emerging risks related to virtualisation in that the clients need to be aware of such as hypervisor level attacks aiming to gain control over the virtual machine manager in order to subvert the virtual machine's normal operations. These can can only be managed by the CSPs by maintenance of logs of performance or incidents such as security threats or service limitations.

Compliance risks: Some cloud users must demonstrate compliance with industry standard or regulatory requirements, possibly by undergoing certification. This process might be impacted by the migration to cloud. Indeed, for a cloud user, undergoing a certification would likely require the need for the CSP to provide evidence of its own compliance with the relevant requirements including possibly the need to extend the audit to the CSP. Hence the possibility of achieving security-related certification depends also on the CSP. Certification passed before migration to a cloud solution might lose value once migration takes place.

Management interface compromise: Public clouds which are accessible via the internet are subject to the same vulnerabilities as the ones inherent to online activities e.g. web browser vulnerabilities.

[59] ENISA (2012) Procure Secure: A Guide to Monitoring of Security Service Levels in Cloud Contracts.

Insecure or incomplete data deletion: When a cloud user decides to remove some data from the cloud, it is unclear how the user can ensure that the data have been really deleted.

Malicious insiders: the management of cloud architecture necessitates the granting of privileged access to technical staff in the CSP. These roles present a high risk as they might be able to get access to customer data in some settings. A strict control of role attribution, access rights and privilege management are essential to prevent attack from inside the CSP.

The forthcoming Commission initiatives on security, eAuthentication and standardization will also cover cloud service provision. The European Strategy for Cyber Security will consider legal and non legal proposals to improve the security of networks and information systems and user take-up of information security risk management practices. As regards the cloud aspect the key issues at stake include:

- The establishment of common network and information security requirements for market operators by extension in relation to data breaches. Cloud service providers would need to take appropriate technical and organizational measures to manage the risks posed to their systems. The development and adoption of industry led standards, technical norms and security-by-design principles that enable users to evaluate in a simple manner the level of data protection and security offered by the provider.

- Promotion of the take up of technical specifications and standards in the field of cloud security and authentication

The Commission has proposed a Regulation on electronic signatures and the mutual recognition and acceptance of notified electronic identification schemes across borders. Although reliable authentication in the cloud do not differ from authentication requirements in general, it is important that authentication in the cloud always requires careful credential and attribute management and credential issuance. In the cloud the authentication challenges relate to loss of governance as the chain of the service distributors may be long and include various actors with different functions.

Finally, the regulatory reform on European standardisation (proposal for a regulation on European standardisation)[60] acknowledges that the Commission can recognise technical specifications in the field of ICT, which may be referred to in order to enable interoperability in public procurement. The Commission has set up a multi-stakeholder platform for ICT standardisation, which can endorse ICT specifications for public procurement. The Commission has set up a multi-stakeholder platform for ICT standardisation, which can endorse these technical specifications for public procurement. The technical specifications for cloud will be part of the work of the multi-stakeholder platform in the coming years – especially looked on from the point of view of governmental clouds.

Among other current initiatives, it is notable that ETSI (European Telecommunications Standards Institute) has held a conference, acting jointly with the (NIST) U.S. National Institute for Standards and Technology and has subsequently set up an ETSI Cloud group to consider cloud standardisation needs. The ETSI technical committee on cloud has had 3

[60] The Proposal for Regulation on European Standardisation , COM (2011) 315 is expected to be adopted by the European Parliament in September 2012

meetings, contributed to the NIST roadmap for Cloud standards and liaison with other standards organisations mainly ITU-T and ISO. It has started to work on ecosystem developing and reached out also to other stakeholders in the standardisation field such as Japan GICTF. ETSI also has a conformance test centre capable of determining whether a product conforms to an interoperability standard. Cloud computing will be an important working area in the next year's ETSI work programme.

IT-industry is also actively looking into the standards issue. SAP has launched an initiative on Gold Standard for cloud computing. The standard would focus on user's three key concerns: trust, security and compliance. The golden standard would be EU-wide, consolidate existing standards and take into consideration especially the privacy regulation in the EU.

In the e-Science domain, the European Commission-funded project Siena has undertaken extensive road mapping to accelerate the adoption and evolution of interoperable computing infrastructures.[61]

What needs to be done? Key themes of **standardisation** in the cloud would include:

Public data formats: data created in the cloud should be recoverable and reusable, without loss of information.

Standards need to be identified for the support of user requirements: For example, the recording of data needed to determine whether a Service Level Agreement has been met; or the logging of information to support third-party audit of data access.

Privacy enhancement technologies will be developed and deployed to give users control of data access. These technologies should be the subject of standardisation actions to avoid problem of non-interoperability and lock-in.

For **certification**:

Providers of cloud services should create a (voluntary) certification scheme which enables users to evaluate and compare in a simple manner the level of

- Conformance to standards
- Interoperability
- Data portability

offered by providers. This should be developed into an industry-wide, uniform and simple way of describing conformity through certification.

These schemes should involve all stakeholders: cloud providers, cloud customers, data protection authorities and certification bodies. Certification would also encompass the verification that the provider has implemented the IT security and data protection appropriate technical and organisational measures and the safeguards for data transfers. For example, certifying that a cloud provider has put in place compliance mechanisms as a data controller or as a processor, as appropriate. These certifications could be implemented at a European if not global scale and contribute to existing ICT certifications or audit regimes adapted to the

[61] Siena roadmap for science cloud standards (http://www.sienainitiative.eu):.

needs of cloud services and should promote user control, interoperability and data portability in order to avoid lock-in.

Certified cloud providers may have a competitive advantage vis-à-vis non-certified ones insofar as, in principle, they would offer higher trust and security standards.

In addition certifications should be recognised by public sector, so as to ensure that public sector can trust cloud providers and benefit from the economies of scale that it allows. The public sector can lay down requirements for conformity to standards, interoperability, data portability and certification. It is potentially the leading market with respect to these requirements and can trigger a supply industry capable of meeting both public and the private sector demands in these respects. More specifically, the public sector can act so as to further the implementation of the European Interoperability Framework (EIF), identifying standards interoperability and data portability requirements, as regards public sector cloud-based services.

5.5. Safe and Fair Contract Terms and Conditions of Cloud Computing

5.5.1. Development of model contract for Service Level Agreements

Traditional IT outsourcing arrangements are typically negotiated and related to narrowly specified data storage and processing facilities and services. Cloud computing, on the other hand, offers scalable and flexible IT capabilities according to changes in user's demand. The greater flexibility of a cloud computing service as compared with a traditional outsourcing contract is often counterbalanced by reduced legal certainty for the customer relation to any contract with the provider.

There may be unforeseen costs and risks hidden in the terms and conditions of such services. The use of "take-it-or-leave-it" standard contracts might be an optimal cost-saving solution for the provider but is not always the best practice from the customer perspective. Those Service Level Agreements (SLAs) often fail to address the operational and legal risks inherent in cloud-based service offerings. For example, they are not deliver the right performance outcomes, or might shift many significant risks to the customer.

The Public Consultation Report on Cloud Computing[62] and the results of the study "Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up"[63] underline that the need for model contracts for Service Level Agreements (SLAs) at European level is a widely shared opinion among all respondent groups.

In the public consultations on cloud computing, several respondents underline that model Service Level Agreements will help Cloud services to define the rights and responsibilities of all involved parties.

According to the Industry Recommendation on the Orientation of a European Cloud computing strategy[64] the development of standard Service Level Agreements that define basic

---

62 Public Consultation Report on Cloud Computing, December 2011, available at http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf

63 See: Study "Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up", D3 – Analysis of the demand of cloud computing services in Europe and barriers to uptake, IDC (2012) op cit.

64 See: Industry Recommendations on the Orientation of a European Cloud Computing Strategy, November 2011avilable at:

requirements and criteria might be useful to enhance transparency and reduce the transaction costs in public procurement of Cloud services.

5.5.2. European model contract for consumers and small firms

Under EU law, the conditions and terms of a service should be clearly communicated to the consumer, and the statutory rights of the consumer must be fully respected. Cloud providers must be compliant with the provision of a transparent, available, secure and accountable service. Moreover, the security policy included in the terms of service proposed by cloud providers should be stated in a clear and straightforward way.

Currently, however, individual consumers – user of cloud service have little negotiation power and conclude contracts that do not foresee liability for the integrity of the data; often contracts do not provide for respect of the confidentiality of content or continuity of the service; some of these contracts also impose a choice of applicable law[65] or make it difficult to do data recovery after termination of the service.

Identifying and developing consistent solutions in the area of contract terms and conditions is a way of encouraging wide take up of cloud computing services by increasing trust by consumers – prospective cloud customers.

The respondents of the public consultations on cloud computing systematically state that clear, consistent and customer friendly terms would create an advantage and thus market pressure has moved, and will continue, moving the industry quickly towards consumer` legitimate expectations.

In this context, European model contract terms and conditions could be envisaged.

Existing EU legislation does to a certain extent protect consumers when using cloud services and other digital products, but consumers are often unaware of these rights, including where they have recourse to the court, which law applies to their dispute and find it difficult to get redress in case of problems.

5.5.3. Binding corporate rules

The proposed Data Protection Regulation facilitates transfers to countries outside the EU/EEA while ensuring the continuity of the protection of the individuals whose personal data are transferred abroad. According to Article 41 of the proposed Regulation "the Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection" The proposed Regulation also "codifies" binding corporate rules, permits their application to processors and "groups of undertakings" and streamlines their approval process. It further empowers the Commission to adopt delegated acts for the purpose of further specifying the criteria and requirements for binding corporate rules.

---

http://ec.europa.eu/information_society/activities/cloudcomputing/docs/annex-industryrecommendations-ccstrategy-nov2011.pdf

[65] Such a choice need to comply, however, with Regulation 593/2008

5.5.4. Code of conducts

The Data Protection Directive foresees in Article 27 the possibility of the development of code of conducts intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

Paragraph 3 of this Article states that "draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29". However, such codes of conduct – given the current diversity of data protection rules at national level - may need to be further approved/blessed by national supervisory authorities. This might be one of the reasons for the limited number of Codes of conduct developed so far under the current legal framework. The proposed Regulation also encourages the drawing up of codes of conducts byforesees the possibility for business and stakeholders to contribute to the proper application of the Regulation develop codes of conducts.

In this context, the Commission will support the development by the industry of cloud specific codes of conducts, which then may be submitted of the supervisory authority for an opinion. The Article 38 of the Regulation provides for the and, importantly, empowers ment of the Commission (Art. 38) to decide, via implementing acts, on the general validity within the Union of such codes of conduct.