

**INDUSTRY RECOMMENDATIONS TO VICE PRESIDENT
NEELIE KROES ON THE ORIENTATION OF
A EUROPEAN CLOUD COMPUTING STRATEGY
November 2011**

This report presents key recommendations from a select industry group to the European Commission on the orientation of a Cloud computing strategy for Europe, and proposes some actions for the European Commission and industry.

LEGAL NOTICE

By the Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit.

Neither the European Commission nor any person acting on its behalf is responsible for the use which might be made of the information contained in the present publication. The European Commission is not responsible for the external web sites referred to in the present publication. Reproduction is authorised provided the source is acknowledged.

Disclaimer

This document has been received by the European Commission. It represents advice tendered to the European Commission by external experts. It cannot be considered as representing the opinion of the European Commission or any of its officials.

This document has been drafted on the advice of experts acting in their personal capacity. Opinions expressed here are therefore only informative and have no binding character whatsoever. Where affiliations are mentioned it is for purposes of identification and reference only. Any use made of the information in this document is entirely at the user's risk. No liability will be accepted by the European Commission, the individual experts or their organisations.

INDUSTRY RECOMMENDATIONS TO VICE PRESIDENT NEELIE KROES ON THE ORIENTATION OF A EUROPEAN CLOUD COMPUTING STRATEGY

November 2011

This report presents key recommendations from a select industry group to the European Commission on the orientation of a Cloud computing strategy for Europe, and proposes some actions for the European Commission and industry.

Contents

1. Overview
2. Background
3. Data Privacy, Governance and Identity
4. Trust, Security and Certification
5. Interoperability, Data Portability and Reversibility
6. Innovation and Uptake
7. Key Recommendations and Actions

Annexes

- Annex 1. Recommendations on the Review of Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and the Free Flow of Such Data (addressing Actions I.1A, I.3A, I.7A)
- Annex 2. Best practices for Cloud Providers on Transparency (addressing Action I.3B)
- Annex 3. Draft Proposal to the European Commission for the Creation of a European Cloud Observatory (addressing Actions EC4B, I.6A, I.6B)
- Annex 4. Public Sector Cloud Strategy for Europe (addressing Action I.5A)
- Annex 5. Breach Notification (addressing Action I.7A)
- Annex 6. Feasibility and Modalities of Creating Efficient Industry-led Voluntary Certification Mechanisms (addressing action I.8A)
- Annex 7. Requirements from a Research and Innovation Point of View (contribution to action EC9B)

Annex 8. Comprehensive Inventory of Relevant Existing and Emerging Cloud and Internet-related Standardisation and Interoperability Initiatives (addressing action I.10 A)

Rapporteur

Dr. Eugene Sweeney, Iambic Innovation Ltd.

Contributors

Contributions to this report and the Working Groups were made by representative of the following companies:

Accenture	EADS	Oracle
Adobe	Enisa	Orange FT group
Alcatel-Lucent	Ericson	Panasonic
Amazon	EuroCloud	RedHat
AmCham	Google	SAP
AMD	HP	Symantec
AVG Technologies	Huawei Technologies	T-Systems
BSA	IBM	TechAmerica
Canon	Intel	Telecom Italia
Cisco	Logica	Telefonica
CloudSigma	Microsoft	TU Darmstadt
Dell	Nokia	Verizon
Dassault Systems	Nokia Siemens Networks	
Deutsche Telekom	Open Forum Europe	

INDUSTRY RECOMMENDATIONS ON THE ORIENTATION OF A EUROPEAN CLOUD COMPUTING STRATEGY

1. Overview

Cloud computing represents a continuing evolution away from the decentralised IT systems of the last decade. It is already transforming providers of IT services and it will change the way other industrial sectors provision their IT needs, as well as the way citizens interact with their computers and mobile devices. Cloud computing, although in its early days, is already a commercial reality and the adoption rate of Cloud computing Services is growing.

A 'Cloud' implementation is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service).

The EU needs to become not only Cloud-friendly, but Cloud-active to fully realise the benefits of Cloud computing. The Digital Agenda is Europe's strategy for a flourishing digital economy by 2020. It outlines policies and actions to maximise the social and economic potential of information and communication technologies (ICT's), notably via the Internet. The development of a European Cloud computing strategy is one of the actions of the Digital Agenda.

This report presents recommendations from a select industry group to the European Commission on the orientation of a Cloud computing strategy for Europe, and proposes some actions for the European Commission and Industry to achieve this. It is the result of a series of discussions with a select industry group, initiated by VP Kroes in early 2011. Following an inaugural meeting with the select group on April 27th, Industry Working Groups were established to work on four main areas, which were seen as a critical to address if Europe is to become Cloud-friendly and Cloud-active. These areas were:

- Data Privacy, Governance and Identity Management
- Trust, Security and Certification
- Interoperability, Data Portability and Reversibility
- Innovation and Uptake

Issues relating to these 4 areas are expanded on in Sections 3-6 below.

The Working Groups analysed the issues and identified 10 key recommendations, with related actions to be performed by industry, the European Commission and other actors. The objectives of the actions are to elaborate and further inform the key recommendations, or to support their implementation. The Key recommendations and actions are presented in Section 7 in terms of:

- Legal Framework related recommendations and actions
- Market related recommendations and actions
- Technical related recommendations and actions (including industry recommendations for the EU's research agenda for Cloud computing for the next research programmes)

The annexes to this report contain industry responses to some of the industry actions which have already been addressed by the Working Groups.

2. Background

The continuing development and expansion of the Internet, along with improvements in bandwidth and computing power, in increasingly smaller and lower cost physical packages, means that today's computing and communications systems allow individuals and businesses to access data and processing resources from anywhere, at any time and on any device. We are moving towards the complete virtualisation of resources and ubiquitous access.

Cloud computing is a term that is used to represent the delivery of services and applications remotely. Rather than storing, accessing and processing information at a local computer, data and applications are accessed and processed remotely, from anywhere. Cloud computing, although in its early days, is already a commercial reality and the adoption rate of Cloud computing Services is growing. One study¹ has predicted a Compound Annual Growth Rate of 19.5% in Cloud computing. According to Gartner², the industry is poised for strong growth through 2014, when worldwide Cloud services revenue is projected to reach USD 148.8 billion.

The EU needs to become not only Cloud-friendly, but Cloud-active to fully realise the benefits of Cloud computing. Besides allowing for the provision of Cloud computing in its various forms, the relevant environment in the EU has to address the needs of end-users and protect the rights of citizens. At the same time, it should allow for the development of a strong industry in this sector in Europe.

It has already been recognised that the Digital Single Market is a key driver for productivity and competitiveness in Europe, which will allow firms in all sectors to exploit the potential of ICT that a digital single market would offer. This is even more important for Cloud computing, which by its very nature, operates across national boundaries and across territories with different legal jurisdictions, within and beyond Europe.

There are a number of challenges in this context that need to be addressed to ensure that Europe will maximise the benefits from Clouds. It is important that Cloud computing services can be operated in a way that allows EU organisations to respect their obligations under EU law while reaping the benefits that Cloud computing promises.

- The EU must ensure that it has the right policy framework to mitigate any risks and to seize the full benefits of Cloud computing.
- Technological research is needed if commercial Clouds are to offer guarantees that users expect.
- European ICT Industry needs to focus on Innovation and Deployment in this expanding sector to ensure take-up and use.

Many of the issues raised by the evolution of Cloud computing must be tackled at an EU level or globally; hence it is necessary that a consensus on the way forward is built, leveraging the strength of the EU market and European industry.

¹ Study by PAC Report D2 Figure 3:

http://cordis.europa.eu/fp7/ict/ssai/docs/20090730-d2-eu-ssbs-industry_en.pdf

² <http://www.gartner.com/it/page.jsp?id=1389313>

Four main areas are critical to address if Europe is to become Cloud-friendly and Cloud-active. These were addressed by the 4 industry Working Groups as follows:

Data Privacy, Governance and Identity Management. In a Cloud computing environment, private or commercially sensitive data may be stored, accessed and processed in remote locations, including for example different countries. Thus data protection and identity management become increasingly important to assure continued trust in and uptake of these services. New governance models and processes are also required that cater for the specific issues arising from the inherently global Cloud model of computing. Issues pertinent to this area are discussed in Section 3.

Trust, Security and Certification. Information security is possibly the biggest concern for actual and potential Cloud users. Whilst security frameworks already exist, they are not yet sufficiently adopted across all implementations. Issues which need to be addressed include: compliance, trust and uptake, data security, certification, cybercrime and data breach. These are discussed in Section 4.

Interoperability, Data Portability and Reversibility. One of the most pressing issues with respect to Cloud computing is the need to enhance interoperability and data portability in a market that is rapidly innovating. It is also important to ensure reversibility, i.e. moving data from Cloud to non-Cloud environments. Issues pertinent to this area are discussed in Section 5.

Innovation and Uptake. Actions are needed by both industry and government in order to overcome the barriers to Cloud computing, stimulate uptake and innovation, and so reap the full potential of Cloud computing in Europe. Issues pertinent to this area are discussed in Section 6.

3. Data Privacy, Governance and Identity Management

Trust in Cloud computing is essential if there is to be significant take-up and adoption by end-users, especially when private or commercially sensitive data may be stored, accessed and processed in remote locations, including for example different countries. Many Cloud services involve personal information, some of it sensitive. Thus data protection becomes increasingly important to assure continued trust in and uptake of these services. From an organisational point of view, data protection is also an essential element in data governance.

Governance models and processes need to take into account the specific issues arising from the inherently global nature of the Cloud. Data is subject to specific legislative requirements that may depend on the location where they are hosted, as well as and for what purposes they are processed. Different countries have different laws regarding which kind of data may be hosted where and how it is to be protected. Within the Cloud, data/code may be hosted anywhere within the distributed infrastructure, i.e. potentially anywhere in the world.

Clarification of applicable law governing the flow, processing and protection of data, including requirements for access, use, security and retention is desirable, so that both Cloud users and Cloud providers have a clearer understanding of which rules apply where and how. Among the EU directives and regulations that may impact Cloud services, Directive 95/46 commonly referred to as the EU Privacy or Data Protection Directive is one of the most relevant and important. The Directive 95/46 sets out in principles the common rules related to data protection in the EU as well as rules related to data transfers to third countries. While there is no question that the Privacy Directive, like other EU Directives, applies to Cloud services, questions do arise as to how and to what extent they apply (geographic and potential subject-matter limits), as well as how they *should* apply to maximise the potential benefits of those services, while still providing the appropriate level of personal data protection.

When considering data protection and governance issues, a number of factors and trends are important to consider. Security is an element in Directive 95/46 and currently subject to additional detailed national implementation requirements including, for instance, specifications related to password strength and length. While there is no question that such requirements are well intentioned and designed to improve the practice of privacy in general, their divergence creates unintended and often unjustified barriers to the provision of Cloud services. When considering how to apply the concept of limited divergence, we should promote security without undue imposition of local requirements on national/regional/global deployments of technical applications or innovation related to new services. This necessarily involves EU and global proactive policy efforts to set the conditions for more suitable regulatory frameworks.

Industry also has an important role to play and a number of initiatives are already underway to help foster trust and confidence in the Cloud. One of the most important developments in this area concerned with data stewardship and governance. Providers of Cloud services are not owners of information, but rather stewards, entrusted with information to provide certain services. As such businesses have started developing overall data governance practices. There has been significant work done by a number of organisations to investigate concepts like “accountability” or “Privacy by Design”. Making accountability a cornerstone of corporate governance will help ensure that companies become responsible stewards of citizens’ personal data. The concept of Privacy by Design could be considered as an element of an accountable organisation as the practical implementation of Corporate Governance.

4. Trust, Security and Certification

Despite the efforts by the industry to make Cloud computing safe for end-users in general, the industry needs to build trust in the Cloud market to promote the uptake of Cloud computing as a whole. Information security is possibly the biggest concern for current and potential Cloud users. Cloud users look for security good practices that can be meaningfully enforced in a cloud environment. Whilst security frameworks already exist; for example, ISO security standards, ENISA Assurance Framework, CSA Control Matrix, CAMM (Common Assurance Maturity Model), Cloud use cases are still dynamically evolving. Six key issues need to be addressed: transparency; trust and uptake; data security; methods of validation including certification; civil cause for action against perpetrators of illegal access or interference; and data breaches.

Greater transparency is necessary to provide more insight into Cloud providers' practices.

Trust must be earned with services that are secure and reliable.

Data security, and information security in general, are much broader than just the protection of personal data and extend to, among others, infrastructure resilience, authentication, and related processes. Therefore data security should be treated in its own right and not only in the context of data privacy. Clarity on applicable law concerning data residency and jurisdiction will be essential in governing how organisations, especially those with specific security requirements, will or will not be able to leverage Cloud services.

Certification is a form of validation that, where appropriate, can be an enabler to build trust for end-users through the use of voluntary, industry-led, internationally recognised standards and certification schemes related to cloud solutions. It is preferable for Certification regimes to be internationally recognised rather than regional or national, to avoid a variety of multiple and inconsistent guidelines and certification regimes, which will be costly, difficult to manage, and hence will neither promote trust nor transparency.

Illegal activities affecting Cloud computing environments such as (identity and/or data) theft, fraud and malicious system or data interference are threats to Cloud users and service providers, and can undermine their trust. While the Framework Decision on Attacks Against Information Systems (2005/222/JHA, currently under revision) already requires that Member States impose criminal sanctions on activities including hacking and interference with networks or data stored in computer systems, third-parties and Cloud computing providers have no right of action against perpetrators of cybercrime in most EU Member States. Cloud computing providers could play a more active role against illegal access to their service and data if they were granted a specific civil cause of action against intruders, coupled with meaningful statutory remedies.

Cloud computing providers hold massive aggregations of customer data. Release of these data, whether accidentally or through the action of a malicious third party, can harm customers – particularly if those customers are unaware of the breach. The loss of service continuity and network integrity may be part of breaches in general as well. The current European breach notification regime (introduced recently under the Telecommunication Framework Directive (Article 13a) and e-Privacy Directive (2002/58/EC)) only applies to providers of electronic communication services, thus excluding most cloud providers and other businesses, which does not help to build trust with Cloud users.

5. Interoperability, Data Portability and Reversibility

One of the most pressing issues with respect to Cloud Computing is the need to enhance interoperability and data portability in a market that is rapidly innovating. Concerns are being raised by users that they will not have the ability to easily move their data and applications between different Cloud environments and service providers, or to ensure reversibility, i.e. moving data from Cloud to non-Cloud environments. There is a strong interest to minimise perceived “lock-in” situations, and to ensure data interoperability..

Interoperability is an essential concept for the Cloud to be fair, open and competitive. Developing flexible, common frameworks for interoperability will further support innovation, and help promote the potential underlying benefits of the Cloud itself. Because of the complexity of the hardware/software stack that makes up Cloud computing, it is necessary to explore interoperability and resulting standards on all levels. This ranges from the hardware (server, storage, networking) infrastructure, OS and/or hypervisor level, APIs and related development standards, and formats used to store/retrieve data.

Regulation of interoperability and data portability is premature at this early stage of the Cloud and in light of the market-led initiatives, even though an ongoing monitoring of and participation in these initiatives would be welcome. Initiatives in this area should adhere to the key principles of technology neutrality, global and open standards, and market-led initiatives that are open and collaborative.

Standardisation can help, and there are already a number of Cloud Standards Road mapping efforts already underway^{3,4}. However, the global nature of the Cloud means that efforts should be made to encourage standards which are internationally coordinated with open specifications. A European approach in isolation will in the medium term be damaging for European users and European Cloud service providers. Standardisation should be through market-based, industry driven consensus processes, leading ultimately to a small set of widely implemented, global, open standards for inter-Cloud interoperability including data portability between Clouds (whether public or private).

Greater adoption of Cloud services by governments in a public fashion can both create further leadership by example as well as enhance consumer trust in these offerings. Public administrations need to understand existing standardisation initiatives and define the level of interoperability required by e-Government services in the Cloud.

Greater adoption in a public fashion of Cloud services by governments in general will enhance trust in these offerings, both for public and private users.

³ NIST CCSRWG-056, NIST Cloud Computing Standards Roadmap, Eighth Working Draft, March 10, 2011

⁴ SIENA European Roadmap on Grid and Cloud Standards

6. Innovation and Uptake

A Cloud friendly and Cloud active Europe will provide significant benefits to individuals and businesses, and provide new business opportunities for Cloud service providers. However, to achieve this, take-up is critical and relies on having an appropriate technical and regulatory infrastructure, with a supportive policy framework.

The adoption of Cloud computing in Europe is as yet not sufficiently transparent. Most studies have a global scope and do not specifically evaluate the situation in Europe. The term “Cloud computing” is also used differently even to the extent where the boundaries to classical outsourcing services become blurred. Nonetheless, most studies suggest that approximately 50% to 60% of businesses use Cloud computing services today across all customer segments, although these Cloud services are mostly applied to non-core activities e.g. web-based e-mail service or storage resources for backup purposes. The majority of businesses use Cloud services for 25 % or less of core business applications. Surveys have shown that Cloud services awareness in the market is dominated by three Cloud players: Amazon, Microsoft, and Google. The awareness of offerings is one of the primary purchasing drivers.

The most important barriers to the adoption of Cloud computing are data security and business continuity concerns. Trust in Cloud computing is a key prerequisite.

Barriers from a user perspective are:

- Security – Unknown or low compliance and security standards as a major concern
- Reliability – Concerns on availability of service especially for business critical tasks
- Data privacy – The fear of moving sensitive corporate data to the Cloud
- Vendor/data lock-in – Concerns about a perceived dependency on vendors once data has been transferred to the Cloud
- Legal concerns – E.g. regarding the transfer of legal liability
- Network performance - Data transfer bottlenecks; insufficient quality of service
- Lack of awareness – users not aware of benefits of Cloud computing, how to leverage it and the available offerings

Barriers from a vendor perspective:

- Different national regulatory frameworks – Cloud services providers have difficulties to achieve required scale when different rules e.g. regarding data location have to be obeyed
- Business model transformation – Cloud computing requires all ICT companies to change their business model without creating disruption

Actions are needed by both industry and government in order to overcome these barriers and reap the full potential of Cloud computing in Europe. The focus of these efforts should be to

- Foster the uptake of Cloud offerings, especially by SMEs
- Establish suitable framework conditions for the creation of a strong Cloud eco-system for start-ups and smaller vendors in Europe.

7. Key Recommendations and Actions

This section presents the 10 key recommendations from the select industry group to the European Commission on the orientation of a Cloud computing strategy for Europe, and proposes some actions for the European Commission and Industry. They are organised by:

- Legal Framework related recommendations and actions
- Market related recommendations and actions
- Technical related recommendations and actions

Actions to be addressed by the European Commission are prefixed with “EC” and those for Industry with “I”. Those actions which require input from both are pre-fixed “EC/I”. No timelines for implementation are implied (e.g. short, medium or long term).

Reports on the Industry actions addressed by the Working Groups are presented in the Annexes.

7.1 Legal Framework Related Recommendations

Recommendation 1: Promote the Digital Single Market to encourage efficient cross border Cloud Services

Action EC.1A: The EC should foster the creation of EU-wide harmonised and globally interoperable rules. In particular, it should:

- (i) consider the harmonised implementation of all relevant Directives and legislative instruments in the EU and in a global context; and
- (ii) re-visit the Digital Agenda pillar on the Digital Single Market to take Cloud computing into account, and identify those areas in which a fragmented regulatory market has the greatest impact on the uptake of Cloud services.

Action EC.1B: The EC should conduct an economic analysis that quantifies the potential value add of Cloud services to EU growth and the opportunity cost of those services either not being developed, provided or used in the EU due to unnecessary regulatory barriers, administrative burdens and choice of law/application of jurisdictions issues. This study could also usefully analyse the European Cloud eco-system: players, business models, current strengths and weakness as well as future focus areas for growth, innovation and job creation.

Action I.1A: Industry should provide an overview, based on their experiences in the marketplace, of key obstacles and accordingly which rules need to be harmonised to establish a truly-functioning single market for cross-border Cloud services in Europe⁵.

⁵ See Annex 1 for a Working Group report, detailing obstacles and related rules which need harmonization.

Recommendation 2: Analyse existing legislation and legislation under review to remove barriers to Cloud computing

Action EC.2A: The EC should undertake a more systematic exercise of existing legislation and regulation to identify Directives, national implementations of Directives or national/local laws that might prevent or unnecessarily impair the creation of Cloud industries, the provision of Cloud services or the potential to innovate new business models and technical applications that leverage the Cloud.

Action EC.2B: the European Commission should assess the existence of potential gaps in existing laws or in legislative instruments that are under review or scheduled to be so shortly. In particular, this should include: intellectual property legislation; cybercrime; lawful access to data; legislation affecting B2C relations in the Cloud remains consistent with the free movement of Cloud services in the digital single market; and, authentication rules as part of the review of eSignatures Directive.

Action EC.2C: The European Commission should ensure that the current regulatory framework contains a clear distinction between Cloud computing services and the connectivity services that are supporting them, for the sake of clarity and regulatory certainty; allowing new business models to evolve and take into account the necessary security levels associated with the service.

Recommendation 3: Ensure privacy legislation is horizontally assessed for its compatibility with Cloud computing, and is looked at in a global context.

Action EC.3A: The EC should ensure the review of the Data Protection Directive delivers a result that facilitates Cloud computing in Europe and at a global level and consider the impact of the national implementations of the Data Protection and ePrivacy Directives on the Cloud.

Action EC.3B: The EC should work with other jurisdictions/regions to develop interoperable requirements that facilitate information flows with appropriate security and privacy protection, including the opportunity to build upon recognised existing global initiatives.

Action I.3A: Industry should develop a concrete proposal on how existing European data privacy laws and practices should be adapted to leverage the benefits of Cloud computing while maintaining the level of data protection for users and to work with the European Commission on the review of existing legislative instruments⁶.

⁶ See Annex 1 for Working Group proposals addressing data privacy laws and practices.

Action I.3B: Industry should propose best practices for Cloud providers on transparency, especially as regards their commitment to privacy rules, data handling and data storage⁷.

2.2 Market Related Recommendations

Recommendation 4: SME Cloud Strategy: Raise awareness and encourage uptake of Cloud computing

Action EC.4A: The European Commission should support the development of Cloud computing seminars for SMEs; provide an EU stakeholder platform (e.g. Thematic Network or Best Practice Network) for the initiative under the EU Competitiveness and Innovation Program (CIP); and encourage Member States to leverage EU Structural Funds to support awareness raising and uptake of Cloud computing.

Action EC.4B: The EC should Foster the Creation of a strong European Cloud ecosystem, through the creation of a European Cloud observatory, in the form of a website (with related social media)⁸

Action I.4A: Industry should promote outreach to SMEs and relevant trade associations from the supply and demand side. Concrete steps should be undertaken for outreach to, and inclusion of, SME players or their representative associations to participate in this initiative.

Action I.4B: Industry should lead initiatives to raise awareness, provide training, etc – which may also include Public Private Partnerships. They should Work closely with SME trade associations, training institutes and other relevant stakeholders to develop curricula for Cloud computing training seminars for SMEs; these seminars should be technology and vendor neutral. Provide industry experts that could teach in such Cloud computing seminars for SMEs.

Recommendation 5: Public Sector Cloud Strategy for Europe: Raise Awareness & Promote uptake of Cloud computing among public authorities.

Action EC.5A: The EC should put Cloud computing high on the agenda of the next eGov Ministerial Conference (November 2011, Poznan, Poland).

Action EC.5B: The EC should develop with member states a coherent public sector Cloud strategy for Europe.

Action I.5A: Industry should work with the European Commission and the member states to develop a European public sector Cloud strategy, especially by proposing Cloud use case scenarios in public sector (local, regional, national, pan-European) and advising on available Cloud technologies⁹.

⁷ See Annex 2 for a Working Group proposal addressing best practice for Cloud providers on transparency.

⁸ See Annex 3 for a draft Working Group proposal for a European Cloud observatory.

⁹ See Annex 4 for the Working Group proposals for a European public sector Cloud strategy.

Recommendation 6: Advance Practices and Contracting in Cloud Computing

Action I.6A: Industry should create a dialogue platform with all stakeholders, including with governments, business users and consumer associations⁸.

Action I.6B: Industry to discuss ways to improve transparency of Cloud providers as regards complex documents and business offerings.¹⁰

Recommendation 7: Ensure a proper response to data breaches in the Cloud.

Action I.7A: Industry to consider warning/notification frameworks for Cloud breaches. This work stream should input as appropriate into ongoing legislative discussions, such as the Privacy Directive Review.¹¹

Recommendation 8: Investigate further the creation of voluntary and industry led mechanisms of enhancing trust and security

Action I.8A: Industry to investigate the feasibility and the modalities of creating efficient industry led voluntary certification mechanisms, taking into account the variety of Cloud business models.¹²

2.3 Technology Related Recommendations

Recommendation 9: Build on the Past & Foster Collaborative Research in Cloud Computing

Action EC.9A: Adequate EU funds should be allocated to collaborative Cloud research and pilot projects, whereas those projects should not be limited to technological aspects but also include issues related to Cloud-based business innovation, education and awareness raising. EU funded Cloud pilots and infrastructure should be expanded beyond eGovernment purposes.

Action EC/I.9B: The EC and Industry together to develop a comprehensive EU research agenda for Cloud computing for the next research programmes¹³

Recommendation 10: Foster interoperability and data portability in the Cloud

Action EC.10A: European initiatives relevant to technology standardisation, including the Commission's on-going reform of the IT Standardisation Framework, should reflect the following principles: Endorsing technology neutrality and promoting competition; Avoiding mandated standards or preferences that could frustrate, rather than promote, on-going and emerging interoperability efforts of the industry at large and among the vendors providing Cloud services and solutions.

¹⁰ See Annex 3 for a draft Working Group proposal for a European Cloud observatory, which also addresses actions I.6A and I.6B.

¹¹ See Annex 1 and Annex 5 for Working Group reports on this action item.

¹² See Annex 6 for the Working Group report on the feasibility and modalities of certification mechanisms.

¹³ See Annex 7 for the Working Group setting out the industry viewpoint on the Cloud computing research agenda for the next research programmes.

Action I.10A: Industry to make a comprehensive inventory of relevant existing and emerging Cloud and internet-related standardisation and interoperability initiatives around the world by governments and industry to ensure this issue is approached in a global manner and to analyse jointly with all stakeholders (demand and supply, including consumers) what improvements can be made in terms of transparency and efficiency of process.¹⁴

Action I.10B: Industry to develop, after assessing existing efforts, a roadmap that identifies necessary steps required moving forward to ensure data portability in the Cloud, and guidelines for ease of migration, as appropriate and taking into consideration the variety of Cloud business models, user requirements and the fact that the roll-out of these steps should take into consideration the ongoing work being undertaken in existing organisations.

¹⁴ See Annex 8 for an inventory of relevant existing and emerging Cloud and internet-related standardisation and interoperability initiatives.