

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 Action Items I.1A, I.3A and I.7A)

14 November 2011

This paper elaborates three of the Industry Action Items (Action Items I.1A, I.3A and I.7A) from the recommendations which the Select Industry Cloud Computing Group submitted to the European Commission in July 2011. It also provides comments and suggestions relating to the review of Directive 95/46/EC, from the perspective of what needs to be done to encourage the development and uptake of Cloud computing in Europe.

Action Item I.1A: Industry to 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 Europe

1. Lack of harmonisation creates substantial impediments for business. These issues are especially important for services based on Cloud computing as they most often rely on cross-border data flows and also derive benefits from economies of scope and scale. The greater the regulatory differences among countries in terms of how data is defined, maintained, processed, secured or deleted; the greater the variety of types of filings related to collection processing, use or storage of data; the more divergent or granular the limitations on collection, use or transfer of data - the more limited the benefits derived from or opportunities for Cloud computing.
2. The gating question is how any organisation develops a website or service that serves multiple jurisdictions while enabling compliance across diverging EU Member State, not to mention global, requirements.
3. 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.
4. Lack of clarity on the intersection between different European Directives, notably the provisions of liability limitations for Internet intermediaries for cases of third party privacy infringements.
5. Lack of clarity on the definition of personal data, the proportionality test and its application to pseudonymous data.
6. Variation across EU Member States implementation of Directive 95/46:
 - a. Different definition of security, and different security national laws.

- b. Over-specification of security elements, such as requiring 8 digit alphanumeric pass codes.
 - c. Variation in data collection requirements. National limits to the free movement of certain types of data.
 - d. Prohibition for certain data to leave the national jurisdiction.
 - e. Requirement for data to be processed by organisations staffed by local nationals.
7. Variation across EU Member State DPA interpretations of privacy:
- a. Availability of BCRs as an option.
 - b. Registration and filing requirements.
 - c. Impact of additional national requirements to legitimise international data transfers in cases where the organisation is already deploying EU recognised methods such as the US-EU Safe Harbor Agreement and Model Contracts.
8. Variation across EU Member State implementation of cookies related requirements of e-Privacy Directive – UK ICO, the Netherlands cases in point:
- a. Diverging required characteristics for consent (“prior”, “explicit”, “informed”, etc.) different approaches to the exact same technologies (e.g. browser settings).
 - b. Variation across EU Member State compliance interpretations like Germany on US-EU Safe Harbour.
 - c. Sub national legislation.
9. Divergence in approaches to data retention periods.
10. Impacts of divergent sectoral laws/national implementation of other Directives:
- a. Restricting processing of certain types of data to processors certified against or accredited on the basis of a local/national standard.
 - b. National technical requirements on e-signatures which, while adopted to transpose the EU e-signature Directive, serve to significantly impede cross-border identification and authentication.
 - c. Diverging rules and processes for access to data by law enforcement (depending on data location, nationality of the data subject, place of establishment of the data controller, jurisdiction where the processing takes place - also linked with the question of applicable law).
11. It is also important to note the potential impact of national restrictions as justification of more draconian localisation requirements by third countries to locate data and/or servers solely within their borders. While governments have interests in the proper security and governance of personal data, data storage location should be a business decision. Restricting movement of data also defeats the very purpose of Cloud: scalability, flexibility, efficiency.

12. We would also propose the following research be undertaken to better identify the obstacles to deployment or uptake of Cloud services and to develop a better understanding of burdens, administrative and geographic differences, and to facilitate the adoption of Cloud computing. The European Commission should expeditiously:
 - a. provide an overview at EU or national level on both the capacity to do business and the effective protection of data;
 - b. start a systematic exercise 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 which leverage the Cloud;
 - c. conduct an economic analysis which quantifies the potential value add of Cloud services to EU growth as well as the opportunity/ cost of those services either not being developed, provided or used in the EU due to unnecessary regulatory barriers and administrative burdens.

Action Item I.3A: Industry to 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 instruments

1. As has been outlined above, Cloud services (both business and technological) operate both within and across borders and are predicated on the ability to transfer and share data, some of which may be personal data. Directive 95/46 has been the EU-wide regulation that outlines compliance obligations related to the collection, use, storage, transfer and deletion of personal data. It is the belief of this working group that the following recommendations can provide solutions that optimise the creation of a framework for the beneficial and responsible information flows that are needed to support the information society and digital economy.
2. The initial part of this paper focused on recommended approaches to privacy and general considerations in review of 95/46. The following are our more specific guidance and recommendations for changes to the Directive. Where possible we have described specific elements of our requirements. We note that while these issues are all extremely relevant to Cloud, they are not unique to Cloud. As such, we have phrased our recommendations so as to address the Cloud requirements in a way that is also more broadly applicable.
3. Before getting to specifics, business is often quoted as calling for greater certainty, but misunderstood as to their meaning and intent. The request of business is not for greater detail and prescription, which often results in needless limits on innovation and has the potential to create burdens and unintended consequences. Furthermore time is the enemy of such levels of specificity as those documents go quickly out of date with changes in technology and business models. The certainty that business requests is not in further detail, but in uniformity of terms/definitions and their interpretation, implementation and application. A similar action should have comparable results across EU Member States. Limits should be placed on the variation in implementation and interpretation, which is not achieved by excessive detail, but

rather by enhanced harmonisation of approach, operation and process. Thus the certainty requested is not in greater detail and definition but rather comparability of implementation, application and result.

4. Specific topics that need to be addressed in the revision of Directive 95/46 include:
5. **Clarification of rules on applicable law.**
6. Cloud will essentially further push the trends that move data from local on-site PCs and servers to equipment which are physically and administratively controlled in numerous jurisdictions. Under the current system, companies that are present in a number of EU Member States often find that they are subject to several different -- and diverging -- data protection regimes. To create greater legal certainty, both for users and providers of Cloud computing, the industry encourages the more unified implementation and clarification of the provisions on applicable law so that each data controller is subject to a single set of rules across the EU. The current approach to applicable law rules might be improved by greater harmonisation of existing approaches to data protection and by introducing a similar “country of origin” principle.
7. It is clear that marked differences in implementations of Directive 95/46 in Member States can create operational burdens and unwarranted administrative hurdles to deploying Cloud services within the EU and serve to undermine the effectiveness of a digital single market. Harmonisation of applicable law requirements whether achieved through member state action or EU regulatory direction would move us significantly towards achieving a “country of origin approach” to determine how and which law to apply in what remain complex legal and judicial environments. The “country of origin” could, for instance, then be the Member State where the main establishment of the data controller is located, as was recently suggested by the Article 29 Working Party in its Opinion on Applicable Law. The Article 29 Working Party has also pointed out that this change can only be acceptable if there are no significant differences between the laws of Member States. In pursuing such a country of origin objective, the drafters will need to consider complex issues which must be addressed in the process. Care must be taken not to provide improper opportunities for forum shopping or regulatory arbitrage and not to disadvantage consumers in the pursuit of compliance or enforcement.
8. Industry notes, however, that there are still unresolved issues relating to applicable law with respect to data processors, as well as to data controllers based outside the EU and that work should also be undertaken to consider how to apply these concepts beyond the digital single market.
9. Work with other jurisdictions/regions outside of the EU to develop interoperable requirements that facilitate information flows with appropriate security and privacy protection including: bilateral or multilateral international dialogue cooperation with regard to minimum protection levels for the privacy and security of transferred data should be pursued. Cloud computing providers face multiple, and potentially conflicting, laws within and outside the EU, concerning disclosure of the information they hold. Achieving a better understanding of jurisdictional issues is critical and should be tackled through enhanced dialogue.
10. Eliminate, where appropriate, or otherwise simplify and harmonise administrative processes specifically including registration and notification requirements; minimise administrative burdens related to cross-border processing and as well as transfers of personal data outside the

EU. Simplification of the DPA notification system would greatly facilitate the deployment and uptake of Cloud services in Europe and we therefore applaud the Commission's intention to examine simplifying and better harmonising the DPA notice regime, and support the decision to consider a uniform EU-wide registration form that would replace individual EU Member State forms. In conjunction with the introduction of a single registration form, we also would support the establishment of a mutual recognition system under which notification in one Member State would constitute notice in all Member States. Under such a system, Member State authorities would have access to a common data base of registrations, enabling DPAs to efficiently obtain the information they need on processing operations while eliminating redundant filings.

11. **Breach Notification:** This issue is dealt with in a section of breach notification in the final section of this paper.
12. **Clarify Controller and Processor definitions and roles.** The divide between controller and processor will become more complex in a Cloud context. Controller, Processors, sub processors and allocation of functions across a continuum of roles makes some existing definitions less relevant or applicable. More and more data processing is outsourced by the controller to a service provider. Controllers often rely on their service providers to determine the most effective technological solutions to deliver outsourced processing. In fact, service providers sell themselves to their customers on the basis of their technical expertise, and necessarily exercise a certain, but limited, autonomy over the means by which they process data on their customers' behalf. However, by doing so, service providers risk exposure under the current framework to the full compliance requirements of the Directive, a disproportionate burden when considering that the purposes for which they process data are entirely mandated by their customer. It is also not in alignment with the typical practice of sharing responsibilities of the service providers and their customers in commercial agreements regarding such data processing services.
13. Therefore, a more accurate approach to the matter is required. The definition of the controller should be based on the decision of the purposes for which personal data are processed (i.e. "why" the data are processed) rather than the means by which this is achieved (i.e. "how" the data are processed). The control over the reason/purpose for processing is the logical basis for allocating different responsibilities between controllers who are responsible for what and why data is processed and processing parties who deal with how data is processed.
14. Any revisions to 95/46 in this area should not further complicate these definitions by creating overlapping liabilities that cannot be reasonably allocated in agreements among the value chain players. Such lack of clarity could impede deployment of Cloud services in Europe by making the legislative obligations and liabilities more confused and complex to manage and understand.
15. **Clarify the intersection between the e-commerce Directive and the 95/46 Directive.** So that it is clear that while we agree that the provisions of the 95/46 Directive apply, it needs to be clear that they are not obstacles for Cloud computing service providers to benefit from liability limitation protections, when they act as Internet intermediary service providers.
16. **Approaches to new technologies.** Many technologies are used for multiple purposes. *Cookies* for instance have roles in security, non-repudiation, trust, navigation, customisation, convenience features, as well as marketing/advertising. Regulation targeted at one use that may raise concerns of abuse may collaterally and negatively impact other uses. Instead the

regulation should focus on the legitimacy of the purpose, the reasonable expectation of the data subject and the potential harm that could result. Clarity and narrow definition of the concern should inform the development of a tailored solution to minimise the potential for unintended consequences and undue burdens.

17. ***Clarify/harmonise rules related to data retention.*** Directive 2006/24 has failed to bring any harmonisation of data retention obligations for Electronic Communication Service Providers (ECS). Indeed besides the harmonisation of the principle at EU level, so far there is no harmonisation in practice. Against this background it is essential, particularly for pan-European ECS, to ensure further harmonisation on the retention period, types of data to be retained, cost reimbursement etc. Nonetheless, whilst further harmonisation is essential, industry should retain the flexibility on how it implements the obligations - for example data storage (centralised or not), handover procedures and interfaces etc. As the EC reflects on the review of the Directive, based on the available feedback from all stakeholders, there should be no extension of scope but rather a focus on limiting the current Directive to what is necessary.
18. ***Enhance clarity and consistency on the applicable law with regard to government access and privacy protection.***
19. ***Defining Personal data*** in a consistent manner that addresses the functional requirements of today's c and services; greater uniformity in applying the concept of personal data needs to be achieved. Right now, differences in interpretation are contributing to legal uncertainty with respect to a critical aspect of EU data protection law. Greater uniformity in applying the concept of personal data needs to be achieved. In particular, we believe it is important to recognise that in certain circumstances, such as for example ensuring the security of the Cloud in the event of a cyber attack, organisations may have legitimate reasons for processing information that the organisation cannot relate to a specific individual and therefore cannot simply be classified as personal data.
20. ***Risk-based approaches to personal data.*** There are a number of possible solutions to address the appropriate classification and protection of personal data, such as introducing a context based concept of personal data, under which data would be deemed "personal data" only if the relevant data controller can identify the individual to whom the data relate in the normal course of its business. If this is not the case another possibility would be the recognition of new categories of data -- "anonymous data" and "pseudonymous data". The former would refer to data that could never be used to identify an individual; the latter would cover data relating to an individual to whom a pseudonym is attached, such as a code, or alias. Pseudonymous data would be subject to a less stringent set of rules than personal data.
21. ***Exclusion of Business Contact Information.*** Business contact is a specific type of personal data which should be usable in relation to the intended purpose (maintaining/developing business relationships and business operations), without the unnecessary additional burdens of demonstrating an independent legitimate basis for processing. Many Cloud service providers utilise business contact information in connection with the authentication of users. As a consequence, an enterprise customer must often obtain consent for the processing of such data from each employee who will have access to the Cloud service. The Spanish DPA has recognised that categorising business contact information as personal data creates unnecessary burdens for companies and has excluded such information from the scope of personal data in Spain.

22. Security/Technical Specifications

23. Security is a concept, which like privacy is dependent on its context. Security to be appropriately tailored in implementation should be informed by appropriate risk analysis and management. Security is a constant objective that is achieved by an appropriate mix of policy, process, people and technology. For security to be effective it must be tailored to its circumstances (infrastructure, nature of information, use/dissemination of information, etc.) and does not lend itself to a one-size-fits-all solution. Thus overly detailed regulations often result in undue constraints or needless burdens in deploying security. Furthermore, such specificity in regulation makes it too time-bound and subject to early obsolescence.

24. Thus, when considering data protection and governance issues, the right level of guidance is important. 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.

25. Privacy by Design/Default

26. Good governance practices include the concepts of privacy and security by design and by default; “by design” being the understanding that organisations should consider privacy and security as issues and objectives from the inception of projects. This is the concept of “built in”, not “bolted on”. Privacy by design is a process based solution which needs to be tailored to company culture, infrastructure and processes. Many companies have implemented processes from secure design and coding requirements to privacy design processes.

27. “Privacy by default” is different from privacy by design in that it is more focused on the choices available to the user and what the default choice should be. To some the most privacy restrictive choice would be an example of privacy by default, but that is often not the appropriate or logical default for a service offered. A requirement will easily fall out of use if it does not comport with the real experience of users and their reasonable expectations. Thus a proposed default that defeats the very purpose of a service offering is not likely to be adopted. Because of the context sensitive nature of privacy by default it best suited to the interplay between the provider and the user.

28. “Privacy by design” is best implemented through self-regulatory mechanisms rather than by regulation. Self-regulation ensures a flexible response to technology innovations. Furthermore, compliance with mandatory requirements that are implemented in even a slightly different manner in each EU Member State would disrupt the Internal Market and dramatically increase the cost of designing and producing ICT products.

29. “Privacy by design” should not result in technology mandates or specified regulatory outcomes, such as “privacy by default”. Technology mandates chill innovation in new and potentially

more privacy-protecting solutions. “Privacy by design” obligations should also be proportionate to the risks facing consumers and met consumers’ reasonable expectations.

30. **Accountability**

31. During the last three years there was a significant work done by a number of organisations and think tanks to investigate innovative concepts like “accountability”. The first one, which has been defined jointly by representatives from regulators, industry and consumer advocates, is one of the most promising to address some of the Cloud-privacy challenges. Making accountability a cornerstone of corporate governance will help ensure that companies become responsible stewards of citizens’ personal data. It has been already endorsed by major stakeholders at the EU and global level. Additionally accountability will provide to companies the required flexibility to address Cloud challenges while also ensuring legal compliance and effective data protection. There are benefits for data protection and for the development of Cloud computing by trying to ensure that legislative approaches are sufficiently adaptable and provide appropriate administrative incentives in place to ensure an effective take up of accountability among the different compliance best practices used by the industry.

32. Accountability is not only a future oriented concept. Accountability is a principle of the OECD Guidelines, is the foundation of PIPEDA (Canadian privacy Law) and is an essential element of the APEC Privacy Framework. Furthermore, accountability has been put into practice in the EU in the form of Binding Corporate Rules; recognised as such in papers from both the Article 29 Working Group and the EDPS.

33. **Accountability Mechanisms**

34. ***Binding Corporate Rules (BCRs)***

35. Two of the major data privacy constraints of Cloud computing are that personal data are often widely dispersed outside the European Economic Area (EEA) and it is almost impossible to flow down security requirements of each data controller to the Cloud provider. Both of these constraints can be alleviated by adopting a mechanism such as Binding Corporate Rules (BCR).

36. BCRs are a good mechanism to simplify and harmonise administrative requirements and to address concerns that arise from personal data being processed outside the EEA. Under BCR organisations must be able to demonstrate to regulators and individuals that their compliance programs are comprehensive and effective. They accept that they remain liable towards individuals for any infringements caused by their processors that take place outside the EEA and are responsible to provide adequate security. In return, the formalities that are usually associated with transferring personal data out of the EEA (e.g. Model Clauses, submissions to regulators, applications for permits) are much reduced.

37. The current system applies only to data that is processed within a corporate group as a data controller which means that it is currently not available for Cloud providers who process personal data as data processors on behalf of their clients. However, there is no fundamental reason why BCR could not be extended to Cloud providers acting as data processors. It should

be recognised, that efforts are currently underway to develop guidance for processor based BCRs¹

38. **Recommendations:**

39. We recommend that the review of Directive 95/46 explicitly include a provision for BCRs in the resulting framework in addition to currently existing means of data transfer and exchange.
40. We further recommend that the resulting framework expand the concept of BCRs to include processors and organisations that may be part of shared value chains, including those not in the same corporate group . This will extend the utility of BCRs more broadly to Cloud computing providers.
41. A legal basis for BCR and BCR for processors should be introduced into the legal instrument that will result from the Commission’s current review of the legislative framework.
42. The legal basis should enable European Union Member States to allow transfers of personal data across and within groups of companies that have obtained BCR for Processors approval without further recourse to permit applications, prior approval, authorisation or significant formalities. It should be made clear in the legislation that Model Clauses, Safe Harbor or other transferring personal data out of the EEA , while still useful and valid, would not be necessary for companies with an approval for BCR or BCR for processors.
43. The legal basis should be constructed in such a way that Member States can either rely directly on the provision in the European legislative instrument or that they are obliged to repeal or amend any conflicting national laws.
44. The elements of good compliance that an organisation, whether controller or processor, must demonstrate to show that it is an accountable organisation should be clearly set out at a high level in the legislation. Such a list of criteria should include, for example: oversight; leadership commitment; risk assessment; well-documented policies and procedures; training and awareness and monitoring and assessment. These requirements must be written at a high and flexible level that enables them to be appropriately applied to the role and function of the organisation.
45. The Cloud provider’s policies and procedures would have to include the implementation of appropriate technological and operational data security measures.
46. The provisions for BCR for processors should make clear that:
 - a. data controllers who make use of Cloud providers (acting as data processors) with a BCR-type approval would remain liable to comply with data privacy law,

¹ For example the concept of ‘Binding Safe Processor Rules’ (“BSPR”) is under consideration within the existing framework to address this issue. Through BSPRs a corporate group with entities or equipment based outside the EEA will undertake to abide by certain data protection standards in accordance with the same criteria established for BCR but adapted to their role as data processors.

- b. Cloud providers (acting as data processors) should be contractually bound by the data controller to comply with the relevant provisions of the Cloud provider's approved BCR for processors,
 - c. the contract between the data controller and the Cloud provider (acting as data processor) must provide for appropriate oversight, recourse and liability.
47. BCRs remain subject to a review process by the relevant Data Protection Authorities. That process, however despite more cohesive policy direction from the Article 29 working Group, from application to approval, is not sufficiently harmonised in the practices of all Member States and Authorities creating needless burdens for applicants and further exacerbating what might be resource constraints for Authorities. For BCRs or BCRs for processors to work it is important that even more streamlined and centralised mechanisms for application, review and approval be considered including the exploration of more commonly accepted forms and processes and the possible utility of common self-assessment tools in the application process. Furthermore Authorities should also explore whether it may be useful and appropriate to use third party accountability agents to support any aspects of these processes to help address issues of scale should application numbers dramatically increase.
48. **Implementing Concepts of Accountability**
49. Accountability as a concept is welcomed provided that it is a part of a renewed focus on effective Privacy/Data Protection and provided that there are appropriate incentives for organisations to take accountability measures (for example, leniency in case of enforcement). Accountability should not be introduced as a new obligation on top of existing obligations.
50. Instead it should be introduced as an improved mechanism to ensure compliant, privacy respectful, dynamic and burden free flow of information with limited administrative requirements. How each company applies these principles in detail, should depend on the company.
51. More concretely, we suggest the following approach to be used to describe behaviors of accountable organisations. When drafting the actual legislation it needs to be clear that accountability does not replace existing obligations, rather accountability is directly linked to existing EU requirements that are being improved and complemented through the introduction of the following approach. Examples of hallmarks of accountability are provided below by way of tangible examples.
52. The following characteristics are representative of those of an accountable organisation:
- a. Adopting and implementing written policies and procedures regarding processing personal data.
 - b. Assuring at senior management level the appropriate staffing and authority to monitor compliance with its policies and procedures.
 - c. Ensuring that its policies and procedures are put into effect by educating and training staff.
 - d. Putting in place appropriate technical and organisational measures to protect personal data.

- e. Monitoring and assessing the implementation of its policies and procedures through internal validation which may include privacy impact assessments or similar mechanisms as appropriate.
- f. Providing appropriate descriptions of its policies and procedures to the relevant supervisory authority upon request. Those policies & procedures should:
 - ensure responding expeditiously to inquiries, complaints and requests from data subjects to access and where appropriate, to rectify, block or erase personal data the processing of which does not comply with the provisions of this legislation, and
 - provide a recourse mechanism when harm occurs to a data subject due to a failure to comply with its policies and procedures; be proportional to the nature and volume of the personal data that the controller processes, the nature of such processing, and the risks to the rights and freedoms of data subjects represented by such processing.

53. Model Contracts

54. Harmonisation and simplification of model contract procedures. Model contract clauses focus on a data controller's responsibility to ensure adequate safeguards for personal data as it moves around the world. While this is welcome, there are shortcomings with this system. Unfortunately some Member States continue to insist on reviewing such clauses even if the Commission's standard clauses are used without amendment, which leads to unacceptable delays in the implementation of international transfers. The model clause provisions are also inflexible and often cannot be changed without triggering regulatory review. Finally, the model clauses are difficult to use in organisations with many subsidiaries.

55. Self-regulation

56. Self-regulatory mechanisms could play an important role in ensuring strong privacy protections in the Cloud, particularly as data is now routinely moving across jurisdictional boundaries, thereby complicating regulatory efforts by national authorities. Part of that role also includes extending the capacity of, and creating leverage for, resource constrained Data Protection Authorities. But to date, very few industry codes have been developed pursuant to Article 27 of the Directive. We would therefore encourage the EU institutions to take a more active role in encouraging self-regulatory mechanisms by, for example, introducing incentives for companies to agree and adopt such arrangements. Specifically as DG JUST is currently drafting a revised framework for data protection in Europe; the revised framework should remain technology neutral, provide legal certainty and promote innovation and development of Clouds. It should also acknowledge the important role that self-regulation can play in this field.

57. Industry certification/verification

58. Industry led mechanisms for demonstrating and verifying organisations accountability need to be considered. There may be potential roles for self assessment, existing industry standards, trust-mark schemes, accountability agents and third party validators all of which should be explored.

Action Item IN 7A: Consider warning/notification frameworks for Cloud breaches. This work stream should input as appropriate into ongoing legislative discussions, such as the Privacy Directive Review

1. The issue of data breach is certainly not unique to Cloud computing, but remains an important factor to address in the Cloud context as a way of encouraging users, especially individuals and SMEs to trust Cloud services to responsibly secure their information. No information system is perfect, but with both increasing targeted and organised cyber attacks including zero-day exploits and information a key target with cyber criminals increased attempts at gaining wrongful access to personal information through social engineering, organisations must be ever more vigilant to address these threats. Furthermore, no one-size fits all solution will address the myriad issues that that are part of the ever more complex security environment.
2. In this context, policy and legislative frameworks related to data breach should encourage a context appropriate and risk-based approach to security where considerations/defense in depth (multiple layers of security) are taken into account.
3. Policy frameworks should also recognised the role technical security protection measures can play, such as encryption, in ensuring that data which is lost or stolen cannot be accessed. The 95/46/EC Framework Directive should provide for a breach notification obligation for controllers of data. This Directive should also include an exclusion of data that has been rendered unusable, unreadable, or indecipherable through practices or methods, such as encryption, redaction, or access controls that are widely accepted as effective industry practices or industry standards. Such a breach notification requirement will enhance network security and promote robust protection of personal data, thus fostering trust and confidence in Cloud computing offerings.
4. The potential for harm or adverse impact needs to be an important element in defining breach and its related notification requirements.

Where extremely little or no risks exists for wrongful actors to use or access personal data , for example due to the use of technical protection measures, then notification may only serve to needlessly panic data subjects.

- a. Examples could include a lost laptop – that was lost by falling off a ferry at sea, or a stolen laptop with encryption. The attenuated risk of usable access to the information should not qualify these actions as breaches or require reports.
 - b. Other examples may exist within an organisation where an employee inadvertently access a file they are not current working on. Where that access has been identified, such as through the use of data loss prevention technologies, and does not result in use or dissemination of the information and where there is no indication that the employee was intentionally attempting to access such information – there should be no consideration of this action constituting a breach nor any reason for notification.
 - c. Where a breach does have a reasonable potential to result in harm or adverse impact, then notification requirements and processes should be harmonised across EU Member States. Where numbers of notifications or identification of all parties is impractical, electronic means of notification, such as e-mail and web site postings, should be permitted.
5. **Facilitating Research and Needed Outreach (general recommendations):**

6. Fund research on:
 - a. Technologies that enable or enhance privacy (FP7 et seq.),
 - b. Information which can enhance trust, including for SMEs (reputation engines, effective communication, and transparency) (CIP).
7. and fund:
 - a. Related education and outreach campaigns,
 - b. Capacity building, where appropriate.

Annex 2

Best Practices for Cloud Providers on Transparency

(Addressing Action Items I:3B)

Action item I.3B: Propose best practices for Cloud providers on transparency, especially as regards their commitment to privacy rules, data handling and data storage.

Introduction to the recommendation/action item

The development of Cloud-based services provided across borders within as well as beyond the EU markets has raised new challenges in implementing the existing rules on the privacy and security of personal data. In particular, to different degrees depending on whether B2B or B2C relations are considered, more clarity and legal certainty are desirable for providers and users alike to understand:

- which rules should apply (applicable law);
- where they should apply (competent jurisdiction); and,
- how compliance should be pursued (enforcement mechanisms).

One part of the exercise is to modernise the current data protection framework (action item IN 3A). Another part is for end-users to gain visibility over their data in the Cloud in order to understand where it is being processed, by whom, for what purpose, how it is secured, and how related privacy rules are complied with in accordance with their own compliance requirements.

Cloud-based business models are highly diverse, evolve dynamically and can involve several providers of various services from different jurisdictions to deliver a given product to the end-user. This may lead to complex value chains which may occasionally be perceived as insufficiently transparent to the end-users, thereby hampering trust and confidence in some user orientated Cloud-based offerings.

The objective of this paper is for the industry to propose solutions to enhance visibility and transparency in such environments, for the shared benefit of providers and end-users.

Benefits

The increasing usage of Cloud services is a global trend not restricted to local boundaries. Data is routinely transferred across jurisdictions, and various local laws may apply to how it is processed, especially when privacy is at stake. Cloud providers have adopted different approaches and solutions for data governance and related legal compliance, depending on a broad range of factors such as where the service is provided, how and by whom data is processed, whether the end user is a consumer or a business. Accordingly, information made available by providers about the value chain that contributes to the delivery of a given service may vary in scope, level of detail and accuracy,

depending both on the provider's own policies and processes and on the customer's demands and expectations. The suggestions below are made on the understanding that better transparency can be pursued as a business facilitator for both parties, providers being able to better meet user expectations, and users gaining more confidence in Cloud-based offerings. This could eventually improve the uptake of Cloud Computing in general.

Business practices around this subject

Organisations have an interest in offering an appropriate level of transparency and/or assurance that can enhance user confidence and thereby boost business performance through competitive advantage and higher added value. There are various paths towards achieving such superior value, and the kind and level of detail of information required will vary according to the concrete business models considered, and to whether B2B or B2C transactions are considered.

Certification

Currently, to ensure compliance with data security, data protection and privacy requirements when procuring Cloud services, most often business customers can, depending on their requirements, require their vendors to certify against the ISO2700x framework. This certification enjoys global recognition in the marketplace. Therefore, investing in ISO27000 certification is a way for providers in certain fields to add value and competitive edge to their services. However, while an ISO certification is potential one way to build trust with customers, it is technology agnostic and not specific to Cloud computing solutions. Most Cloud providers cover the items on privacy rules, data handling and data storage within their own Service Level Agreements with their customers or depend on existing legislations and regulators. Other initiatives include efforts by the Cloud Security Alliance, as well as the ENISA Cloud Computing Information Assurance Framework and the EuroCloud Star Audit Certification. It should be born in mind that certification generally comes at a significant cost, which may make it unaffordable for smaller organisations. This could be offset by having a clearer understanding of the schemes that exist and their appropriate scope. In this process it should be borne in mind that the need for certification and the type and frequency of certification will vary on the basis of the business model and customer requirements.

Market-based mechanisms

With user demand on the rise, offering visibility and transparency in Cloud value chains particularly for business customers is becoming an increasingly valuable business proposition, whether in terms of providers giving more information about their own supply chain as an added value service, or third party providers offering technologies that enable users to assess; for example, data security measures or IT risk compliance in the Cloud infrastructures they use.

Self-regulation

A particular form of market-based mechanism is self-regulation whereby Cloud providers develop their own transparency schemes (e.g. providing particular information to users, endorsing specific commitments in Service Level Agreements) with a view to achieving competitive edge. In the B2C area where users are often offered off-the-shelf terms of use with a limited scope for negotiating tailored service levels or contract terms, accurate and detailed prior information and – as far as the processing of personal data is involved – consent are legal requirements under the data protection and consumer protection frameworks.

Moreover, specifically in the B2C space, statutory rules may apply to Cloud services on various points such as applicable law and competent jurisdiction (consumer rights directive), contractual arrangements (unfair terms directive), advertisement (unfair commercial practices directive), liability rules related to information society services (e-commerce directive), etc. These matters, covered under law, don't come under self-regulation. Nevertheless, as a matter of transparency and confidence building, Cloud providers targeting the consumer market should pay specific attention to raising consumers' awareness of such legal provisions being applicable, and of the relevant requirements being complied with.

How to proceed

As we consider mechanisms of enhancing transparency, we must correctly take the operational realities of Cloud services into account, ensuring the businesses' continued flexibility, benefits and innovation. Meanwhile we have to find ways to provide users of those services with the information they seek to gain trust in the services and providers.

Going forward, efforts should distinguish between the business and consumer markets, as transparency needs and compliance requirements are both very different in these two areas.

On the basis of this distinction, the group recommends exploring and understanding real current requirements of the respective users (businesses and consumers) in relation to transparency, as well as raising awareness of what factors are relevant for each user category to consider when using Cloud services, ranging from the kind of information consumers should look for, to the compliance and reporting mechanisms that businesses should foresee in their Cloud contracts, etc. This could be done in a form of a study supported by the European Commission in which the relevant stakeholders would be consulted and given the opportunity to provide input.

Based on the results of the study, options and tools to explore in order to enhance transparency could include the setting up of publicly available resources (websites, publications...) to provide specific and regularly reviewed, augmented and improved guidance materials for the different target audiences on the topics of highest interest and relevance to them.

In the B2B area, self-regulation should be encouraged, market-based services geared towards achieving superior transparency in Cloud architectures should be allowed to develop, and emerging practices may then provide a practical basis for undertaking the development of voluntary standards and certification schemes that can pragmatically meet users' demands as well as providers' needs.

In the B2C space, consumer information and awareness raising practices may be explored and encouraged. Own initiatives, commercial or public-private partnerships, as well as industry supported public initiatives (e.g. in the framework of, or similarly to the European Commission's ECC-Net¹) are only a few of the possible avenues.

Moving forward, as best practices emerge in the market place and are validated through user experience, channels for information sharing as well as voluntary benchmarking schemes should also be explored.

¹ European Consumer Centres Network: http://ec.europa.eu/consumers/ecc/index_en.htm

Who to involve

1. Cloud providers and their industry associations to provide the supplier perspective;
2. User organisations (representing businesses, respectively consumers depending on the issues addressed) to provide input on user expectations;
3. Legislative and regulatory authorities to provide knowledge and clarity on legislative and enforcement matters;
4. Organisations pursuing similar objectives in third countries / other regions.

Deliverables

At this stage, the key action items proposed are the following:

March 2012

- mapping actual user requirements in terms of assurance and transparency, distinguishing between business users and consumers;

September 2012

- developing common sets of guidelines for each market segment on what relevant information the respective users should look for and providers could make available to address the legitimate concerns and requirements identified;

from September 2012 onwards

- exploring channels and mechanisms to disseminate that information, the case being by industry, by authorities, by consumer organisations, depending on the target audience considered.

Annex 3

Draft Proposal to the European Commission for the Creation of a European Cloud Observatory

(Addressing Action Items EC.4B, I.6A and I.6B)

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

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

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

To help drive awareness and adoption of Cloud computing in Europe, the Commission could establish an online European Cloud Observatory as an independent repository of relevant information about technologies and best practices.

The Observatory could focus on the evolution of the Cloud industry in Europe, highlight the opportunities for European SMEs as providers and consumers of Cloud services, and help users in all sectors understand and evaluate the potential economic benefits of Cloud computing. One part of the Observatory could be designed for structured dialogue between providers, users and public sector agencies in an effort to increase transparency of practices.

The Observatory could also be the vehicle to support the launch of the EU Cloud Strategy and promote current policy developments.

The Observatory would provide:

1. A central pan-European information platform on Cloud computing which would include news, events, case studies and newsletters about on-going initiatives, projects, new applications and developments in European Members States and across the world;
2. Guidelines, checklists, model use cases to help learn about new and existing Cloud services and relevant policy issues;
3. A repository and registry which would give visibility to European enterprises providing Cloud services, projects and initiatives in public administrations, allowing users to upload and download, search and retrieve public documentation and reviews.;
4. Exposure for Cloud Services created by European SMEs in order to increase awareness of these contributors to the knowledge economy and the types of solutions they provide;
5. References to best practices for deploying Cloud services and for promoting development, adoption and awareness about Cloud Computing for citizens and the local ICT economy;

6. A library of economic studies and related research;
7. Resources for skills training specific to development and use of Cloud services.

How would the Observatory be structured?

The European Cloud Observatory could be a public facing web site with an accompanying member service, open to Cloud practitioners such as decision makers and experts from public administration, academia and industry. Members would be able to publish information about Cloud developments and projects on a national or pan-European level, launch discussion on issues of concern, promote workshops and disseminate information about their own events. This community would aim at being the single point of reference at EU level with regard to Cloud computing.

The member dialogue element of the Observatory, for discussion of issues of concern, could start initially with topics of interest raised during the Expert Group consultation during the course of 2011, in particular with regard to increasing transparency of practices, concepts and models, as well as increasing understanding of common taxonomy. In particular, a platform for questions and feedback regarding the guidelines, checklists, and model use cases mentioned above could assist user understanding and evaluation of Cloud services and in turn increase trust in such services. Often, variations in services and in contracting practices reflect a Cloud business models, and dialogue to increase understanding of the different business models will also help users understand the different types of services.

The creation of the Observatory would be funded by the European Commission, with a budget to be determined for the development and maintenance of the technical platform and supervision of the content – perhaps in conjunction with existing website investments funded by DG Information Society. Staff or a vendor would be needed for management of press releases, the newsletter, blogs, etc.

Industry as well as users would need actively to contribute to the content of the Observatory to make it a successful single point of reference. Industry could commit to a level of content to initially populate the Observatory.

The Commission and industry could use their usual channels of communication and promotion about the Observatory.

Annex 4

Public Sector Cloud Strategy for Europe

(Addressing Action Item I.5A)

Action Item I.5A 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 technologies

1. Need for a European Public Sector Cloud Computing Strategy

Like the private sector, governments and Public Sector agencies have realised that Cloud computing can significantly reduce IT costs and improve the performance in public services. Successful projects show an immediate return on investment, and overall savings from infrastructure, labour and energy costs are estimated at 25-50% at average. The expectation of an immediate fiscal and operational benefit is the main trigger for Public Sector to enhance their business processes with Cloud solutions, or move them completely into the Cloud, especially in light of current budget restrictions. Consolidation of data centres is an important facilitator for the strategy to transfer IT solutions from in-house to an external software provider.

There are promising Cloud projects in several Member States by public agencies at local, regional or national level. In some cases these projects have already led to success stories in terms of costs reductions or a better quality of services. The European Commission has pointed to the potential of Cloud computing for the Public Sector in its Digital Agenda and the recent public consultation on Cloud computing. The Commission has also launched a pilot “Towards a Cloud of Public Services” within the Competitiveness and Innovation Programme (CIP ICT PSP).

However, the uptake of Cloud Computing in the Public Sector in Europe is still slow. Moreover, the various Cloud initiatives in Member States are not fully aligned and coordinated at EU level. Europe lacks a coherent strategy to foster the adoption of Cloud computing in the Public Sector. It should be stressed that a rapid and wide deployment of Cloud services in the Public Sector could significantly drive market development of Cloud computing in Europe. Public agencies are the largest procurers of IT products and services in Europe; their move to the Cloud would drive market penetration.

A closer cooperation among public administrations on Cloud computing in Europe would yield further benefits: It could raise awareness about the benefits of Cloud computing in the Public Sector, address common concerns and generate best practices. Public administrations could support EU-wide standards for Cloud computing that would enhance interoperability and create economies of scale. Another outcome could be the creation of Cloud-based cross-border public services (G2C, G2B, G2G) – key enablers for the realisation of the internal market.

This paper outlines actual and potential uses cases for Cloud computing in the Public Sector at the local, regional, national and cross-border level. The paper also contains a set of recommendations for public agencies and policy-makers on how to overcome actual bottlenecks and to develop sound strategies for the migration to the Cloud.

2. Actual and Potential Use Case for Cloud Computing in the Public Sector

Case studies prove that Cloud technology will only deliver the desired return on investment if it addresses the people and process issues that are needed to manage effective systems. Users – employees or citizens – need to immediately see a benefit. Benefits in this sense can be cost or time savings, a reduced workload, improved quality of service, better usability or convenience, to name just a few. The selection of scenarios and solutions for a Cloud deployment should always go alongside this potential for improvement.

With security being one of the major concerns in Public Sector, the Cloud deployment will preferably indicate a private or (Government) community Cloud rather than a public Cloud. But this is just a very generic rule and needs to be evaluated in each case: experienced private service providers may actually apply much higher standards than some Public Sector organisations with small IT departments and less expertise.

Virtualisation of the technical infrastructure

A main trigger for Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) is the cost saving effect. The ability of Cloud Computing to perform complex computing tasks cheaply is often cited as the main draw. Data centres are on the rise everywhere in the world, sometimes even to be consolidated to reduce their increasing number. In countries like Germany, Austria or Denmark, we find a well established structure of data centres that host software for Public Sector organisations, especially local agencies. Virtualisation of the technical “backbone” is a relatively easy way to add the advantages of a Cloud deployment to these hosting services, especially the elasticity of a Cloud. Manually or even automatically distributed workloads help to cover peak loads without a disruption of public services.

Cloud services for server storage and backup, web hosting, or processor capacity have been widely and successfully deployed in both private and Public Sector. Public Sector organisations will benefit from a data centre consolidation with Cloud services. This is especially interesting at the local level. On a regional or national level, Public Sector organisations may also act as IaaS provider, for example to smaller cities, Non-for-Profit organisations, or even to small businesses.

Platform as a Service (PaaS) includes the provisioning of development and test platform, exchange oriented scenarios such as Master Data Management with distribution into different systems, Portal (for peak times as in the forerun of political elections), Business Process Modelling tools. All these tools are already widely used in the private sector and should be leveraged by the Public Sector as well.

Productivity Tools

Another standard and proven use case for Cloud services are so-called productivity tools such as email, collaboration tools, messaging, web conferencing, etc.

Government organisations on all levels either replace their email system with Cloud-based email applications. Employees can immediately benefit from additional tools that come with these Cloud applications. For organisations with many locations web conferencing tools are an interesting start into the Cloud experience. Case studies from the US show an immediate return on investment, freeing resources from IT maintenance to more strategic tasks, and giving employees better working conditions.

Collaboration

Collaboration in the Cloud enables employees in different departments, locations, organisations, or countries to jointly work on projects and align their activities. External contributors can be invited to join the group or project. The collaboration increases speed, responsiveness and service quality. Potential use cases include political and governmental decision making, social or crisis intervention, environmental and infrastructure planning projects; alignment of actions with external stakeholders such as scientists, doctors, NGOs, or companies, disaster management, and many more.

Other scenarios might require a home-grown collaboration infrastructure, especially in security critical situations on a national or international level: disconnected entities need to work together, and Member States may have their own discrete IT network but need at least some degree of interoperability on a daily basis.

Information and Transparency

Cloud computing is an excellent way to grant access to information and databases, and increase the transparency of the political process. As long as the information is anonymous there should be concerns with respect to data privacy. Potential use cases include geospatial information, information about public funding streams or statistical information. This is of relevance to all Public Sector organisations including national and European Institutions.

Service and Case Management

Citizen Services, or other external services, are mission critical to many Public Sector organisations. Responsiveness and service quality are carefully monitored performance benchmarks. A CRM system helps to channel and route service requests. In combination with a case management system it creates transparency to the citizen and the employee and helps monitor the status of a cause. Especially for smaller governments a CRM system in the Cloud is an excellent option to improve the service quality at relatively low costs. Ideally, the provider offers sufficient customisation to support Public Sector processes and customer specific requirements. A seamless integration into the local backend would support the process really end-to-end.

Public Sector Specific Applications

All mission critical processes that can be fully or partially standardised can be moved to the Cloud (presuming that data privacy, security, and operability are ensured). This includes

- ERP software such as Financials, Budgeting, HR, Asset Management but also the “core” processes of every administration. Especially smaller Public Sector organisations would not be able to afford a large software implementation on premise. With a Cloud deployment they get access to prime standards, which in the end also improve performance.

- Algorithms within a solution that require intense maintenance and update, such as rules engines for tax assessments, calculations. These parts within a software solution would be maintained centrally in a Cloud while the sensitive data are still kept on premise in a secure environment.

Of course, a certain degree of configuration must always be granted.

Smart City Management

Cloud Computing can be a very effective tool for Smart City Management because the Cloud enables information sharing across all city agencies and departments and the coordination of cross-agency resources to respond to issues rapidly and effectively. The Cloud can significantly increase the quality and effectiveness of city operation management. Executive dashboard capabilities give decision makers a real-time, unified view of operations so they can see who and what resources are needed and available. Cities can rapidly share information across agency lines to accelerate problem response and improve project coordination. By providing visibility into key performance indicators (KPIs) and trends, the Cloud can also help fine-tune current resource usage and support forward-looking planning activities.

Shared Services

The Shared Services Cloud offers government agencies – local and national - the opportunity to lower IT costs while improving performance, security and services. Currently, government agency data is usually managed and owned by individual departments, which can slow cooperation between units as well as the response to citizen needs. Leveraging the Cloud environment to improve application integration can give government managers an overall view of agency operations, issues and services. In particular, the Cloud allows local governments and municipalities to enhance their community service.

School in the Cloud

Some case studies show great success regarding the implementation of a Cloud based platform for schools. In one case study, the Cloud solution has replaced some hundreds of on premise applications and hence, has reduced IT complexity, costs and maintenance needed for these educational programs.

3. Recommendations

For a successful migration into the Cloud, the right timing and the right motivation are essential. Successful case studies show that the following framework conditions provide incentives for a Cloud deployment:

- Fiscal pressures (IT budget, maintenance effort, staff reduction/retirement)
- Imminent replacement or upgrade of IT infrastructure (hardware or software)
- Agile adoption of innovations and changing policies/regulations
- Improved usability or extension of existing services (mobile and remote access, mobile enterprise solutions, graphical displays and geospatial information, Social Media, collaboration and other productivity tools)
- Security concerns and delegated disaster recovery

- Data centre consolidation, optimisation of infrastructure across agencies for economies of scale
- Operations acceleration, service responsiveness, and collaboration, especially across agencies

Against this background we would like to put forward the following recommendations to public agencies as well as the European Commission and Member States.

a) Recommendations for the European Commission and Member States

The European Commission and Member States can provide the necessary framework conditions both at national and European level to foster the adaption of Cloud computing in the Public Sector:

The EU should put Public Sector Cloud Computing high on the political agenda. It should not only be priority of the Digital Agenda and the upcoming EU Cloud Strategy. Cloud computing must also become a cornerstone of the EU eGovernment strategy. It should accordingly be addressed at eGovernment Ministerial Conferences and other relevant platforms. Cloud computing should also be a core element of the eGovernment Action Plan. Ideally the EU and Member States should agree on firm targets for the adoption of Cloud Computing in the Public Sector and on a roadmap with clear measures, milestones and deadlines on how to achieve those targets.

The European Commission and Member States should create a platform to share and develop best practices for Cloud computing in the Public Sector. This platform should envisage regular meetings of government officials and experts as well as an online Cloud computing best practice portal that should be accessible to all public agencies in the EU. The portal can address issues related to available technologies, SLAs, data portability, liability and security requirements. Furthermore, the platform could be used to issue awards for innovative Cloud projects and early adopters of Cloud computing in the Public Sector. The platform could be linked or integrated into the proposed European Cloud Observatory.

This platform could also create an EU-wide Cloud procurement guide for public agencies, similarly to the Cloud Buyer's Guide that has recently been launched by the Cloud2 Commission in the US. This guide would address frequently asked questions and the critical steps that agencies need to consider before making Cloud procurement decisions. The Cloud procurement guide for public agencies could be developed at European level since the challenges for migrating to the Cloud are similar across the EU. The guide should be accessible online for all public agencies. It should be updated on a regular basis to take into account technological progress, new best practices as well as new issues that may arise.

Member States should define standards and regulations to provide reliable guidance to public agencies on how to comply with data security and data privacy obligations in the Cloud. The lack of clear guidance in these areas is the major bottleneck in the Public Sector for the uptake of Cloud services and the development of Cloud best practices in Europe. Especially smaller public agencies will benefit from standards and regulations that would ease their concerns about liability and compliance in a Cloud environment. The standards and regulations should at much as possible being harmonised at EU level. ENISA should continue to providing guidance and fostering an open dialogue with all stakeholders on security issues related to Cloud computing.

With respect to interoperability it is recommended that the Public Sector relies on industry driven standardisation. The IT industry has already produced many standards for Cloud computing and is working hard to close existing gaps in order to foster interoperability for Cloud services. It is important, however, that the Public Sector defines its specific interoperability requirements that should then be taken into account in the standardisation process. Finally, we do favour global standards for Cloud computing rather than regional or national approaches.

Governments should also provide suitable budgeting rules for the procurement of Cloud computing services. Today IT procurement budgets derive mainly from capital expenditure accounts, which often restrict the ability of agencies to procure IT as a service. Public agencies find it especially difficult to predict the costs of Cloud services in a fiscal year and move funds from capital expenditure accounts to the operations accounts. We therefore encourage Member States to adapt current IT procurement models to provide public agencies with the flexibility to procure Cloud computing services.

Finally, the EU as well as Member States should provide public funding to promote the migration of public administrations to the Cloud. Accordingly, Cloud computing in the Public Sector should become a priority of the next multi-annual financial framework (2104-2020), especially within the Connecting Europe Facility Program. It should remain a priority under the CIP IST PSP and EU research policy.

b) Recommendations to Public Agencies

First and foremost, public agencies should develop a clear roadmap into the Cloud, starting with existing services and then take leadership on future services. Agencies should begin with developing a business case that outlines their requirements and performance objectives. The business case will then determine the appropriate Cloud deployment model (public, private, hybrid, or community).

Public agencies could also take into account Cloud services that have already been successfully and widely deployed by other governments or in the private sector.

As with any IT public procurement, public agencies should choose Cloud providers based on objective criteria such as reliability, performance and the total cost of ownership. In particular, public agencies should rely on suppliers that have a track record of providing secure and reliable services.

It is essential that “moving a solution into the Cloud” does not mean “losing control over the IT solution”. Although Cloud solutions involve a natural standardisation they should also allow a customer-specific configuration.

Agencies should also consider the ability of the Cloud applications to integrate with on-premise applications and ensure a seamless end-to-end process where needed.

Public agencies should carefully negotiate the service level agreements (SLA) with the provider of the Cloud service. Smaller agencies often need guidance with respect to negotiating SLAs. Accordingly, the development of standard SLAs that define basic requirements and criteria might be useful to enhance transparency and reduce the transaction costs in public procurement of Cloud services.

The industry can provide support and guidance to build a business cases, assess Cloud readiness and develop a roadmap for the migration to the appropriate Cloud model.

Annex 5

Breach notifications

(Action Items I.7A)

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

1. Introduction on the recommendation/Action Item

The 95/46/EC Framework Directive should provide for a breach notification obligation for controllers of data. This Directive should also cover an exclusion (or ‘safe harbour’) of data that has been rendered unusable, unreadable, or indecipherable through practices or methods, such as encryption, redaction, or access controls that are widely accepted as effective industry practices or industry standards. The breach notification requirement will foster trust and confidence in Cloud computing offerings.

2. Why is it necessary/Benefits

Data breach notification is just as applicable to Cloud computing as to the eCommunications (Telecoms) sector (where there is already a law). I.e. the lack of provision for “information society services” is an omission which cannot be justified.

A breach notification obligation for controllers of data under the General Data Protection 95/46/EC Framework Directive, if properly implemented, can serve as an important instrument to enhance network security, ensure robust protection of personal data, incentivise data controllers to enhance the protection of data subjects. It would create a more efficient market in security. People can make choices on the basis of historical information on breaches, thereby creating market pressure on providers to improve security.

However it is important to note that for a data breach notification system to be effective across all sectors it must be workable and avoid imposing unmanageable burdens on national authorities, businesses and data subjects alike.

Prevent excessive notification: Not all breaches are of equal importance. Some create great risks of harm to consumers from identity theft and fraud, while other breaches create little to no risk. Over notification is likely to confuse Cloud computing users, or any data subjects, who will then fail to take appropriate action when they are truly at risk due to “notification fatigue”. This also may weaken any positive market pressure to improve security measures, which relies on consumers making choices based on historical breached data. We believe notification should be required only in those instances

where an unauthorised disclosure presents a significant risk of harm. **Furthermore a risk-based notification principle** can also create an incentive for businesses to implement stronger data security.

Specifically we recommend:

Exclusion of data that has been rendered unusable, unreadable, or indecipherable: data should not be subject to a breach notification requirement if it has been rendered unusable, unreadable, or indecipherable through practices or methods, such as encryption, aggregation, or access controls, which are widely accepted as effective industry practices or industry standards. These conditions will ensure that data that has been illicitly obtained cannot actually be used to defraud or inflict harm on data subjects. As the apparent breach would not pose a risk to the consumer, it should not require notification. Such an exemption would also be technology neutral and flexible, allowing innovators to continue to develop new techniques and methods without fearing that legislation and regulations have favoured one type of measure over another. It should be noted that even in the case that encryption or access control have been applied, certain additional conditions must be met in order for this exemption to be valid. In the case of encryption, it must be ascertained with reasonable certainty that secret keys have not been disclosed. In the case of access control, it must be ascertained that access credentials have not been compromised.

Clear Definition of ‘adverse effects’: A clear definition of ‘adverse effects’ is needed as not all type of data¹ breaches will cause damage to individuals. We believe notification triggers should focus on substantive outcomes by following a risk based and context orientated approach and entity or group internal disclosures should be explicitly excluded. Where little or no risk exists for wrongful actors to use or access personal data, for example due to the use of technical protection measures, notifications may only serve to create notification fatigue data subjects.

- (a) Examples could include a lost laptop – that was lost by falling off a ferry at sea, or a stolen laptop with encryption (and securely stored keys). The attenuated risk of usable access to the information should not qualify these actions as breaches or require reports.
- (b) Other examples may exist within an organisation where an employee inadvertently accesses a file they are not current working on. Where that access has been identified, such as through the use of data loss prevention technologies, and does not result in use or dissemination of the information and where there is no indication that the employee was intentionally attempting to access such information – there should be no consideration of this action constituting a breach nor any reason for notification.

Awareness Raising: A lot can be achieved by raising consumer and industry awareness of the risks to personal data, and how consumers and businesses can better protect their data and data systems. Data Breach Notifications can help in this process. Many companies have developed their own substantial programs to convey these messages, and many offer free security check-up tools. Industry, consumer groups and European and National authorities should work together to develop awareness raising campaigns on good ‘cyber-hygiene’ and data security risks.

3. What initiatives are already out there

The introduction of a pan-European breach notification regime in 2009 as part of the e-Privacy Directive (Article 4) is the most important initiative of this kind known at present. This legislation

¹ “data” as defined under 95/46/EC Directive

extends to telecommunications providers at the exclusion of other businesses, both on- and off-line. Germany has introduced a sector wide national data breach notification requirement in September 2009 as an amendment to its Federal Data Protection Act (FDPA).

4. Are there best practices around this subject?

To date we are not fully aware of any particular instance of application of the pan-European breach notification regime adopted in 2009. ENISA is currently preparing guidelines on the implementation of Article 4 of the e-Privacy Directive and has an expert working group working jointly with Article 29 and the European Commission, which is open to participation from industry. The deliverables -- including technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred in Article 4.5 of the revised e-Privacy Directive -- are scheduled to be published in Q4 of 2011. At this stage ENISA already published an analysis around the subject².

5. How to proceed

The Review of the 95/46/EC Framework Directive and the related consultations present a unique opportunity to extend the similar breach notification requirement that is currently part of the e-Privacy Directive to other data controllers.

A breach notification measure could be proposed during the Review of the 95/46/EC Framework Directive, requiring all data controllers to provide notice in the event of a breach affecting personal data. The Framework Directive currently includes a security of processing provision that requires data controllers to implement appropriate measures to protect personal data from “accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access ...” (Article 17(1)). The breach notice requirement would be a logical extension of this provision.

6. Who to involve

- European Commission Proposal: lead
- Parliament and Member States
- Industry and other Stakeholders, including ENISA

7. Deliverables (short-mid-long terms in consideration)

Short-term: Extension of Article 17(1) of the 95/46/EC Framework Directive

Medium/long:

- Private-public Awareness effort involving industry and public authorities
- Implementation and enforcement of breach mechanism. Assessment and improvements of the mechanism, if and as necessary

² http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport

Annex 6

Feasibility and Modalities of Creating Efficient Industry-led Voluntary Certification Mechanisms

(Addressing Action Items I.8A)

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

1. Introduction on the recommendation/Action Item

Establishment of a certification standard for Cloud services depending on the needs of the different business models, which is in line with the European and national regulatory requirements on data security and data privacy, and which is a voluntary, industry driven, technology neutral initiative supported by the EU.

The scope of this action item:

- Addresses Cloud services, not Cloud service providing companies as such
- Focuses on commercial Cloud services based on service level agreements (SLAs) offered with standard terms, as they commonly appear with public Cloud services in the field of business to business (B2B) and business to government (B2G) transactions.
- Non-standard SLAs with individually negotiated terms and conditions enable contracting parties to decide directly what proof of compliance or certifications they want to make applicable (typically given in private Cloud scenarios)
- Cloud services offered broadly and free of charge on the consumer market may appropriately be considered for a different analysis in terms of a consumer trust mark or seal.

The certification of Cloud services based on a voluntary, industry driven initiative has to be understood as one initiative to enhance customer's trust in Cloud services, but needs to be accompanied and supported by other trust enhancing measures as well, which are addressed in other industry recommendations.

A certification scheme also required the trust and acceptance of the Cloud service providers. Therefore it has to be carried out by vendor neutral, independent organisations following the agreed and supported audit and certification procedures. It has to be mandatory for them, that confidential, organisational proprietary and non-public security and design information of Cloud service providers involved will be appropriately protected to assure both the security of the system as well as the

continued competitiveness of the organisation. Certification is only really of interest if the certification process is more trusted than the Cloud service being certified.

There is a need to enhance trust in systems through exploring various mechanisms of validation, certification or attestation. These might relate to outcome-based contracts with financial penalties, Codes of conduct/ practice, Transparency and performance publications, reputation, customer retention and other simple market forces. Some customers and providers may be interested in validation or certification via third parties, while different forms of self-certification may also be considered.

It is common understanding that developed certification mechanisms need to be appropriate to the type and nature of the specific Cloud implementation and appropriately take into consideration the potential risks and benefits of the model. These certification mechanisms should strive to provide efficient, cost-effective audit and certification processes that result in credible and comparable information across similarly situated deployments.

2. Benefits

Cloud computing enables a wide range of commercial, operational and procedural benefits for government authorities, for businesses of all sizes and in all market fields. Cloud computing enables, accelerates and widens innovations in all technology fields and leads to a new and different ways of information processing and consumption.

Moreover, by scaling up IT industrialisation massively, Cloud computing contributes to a more efficient energy utilisation and carbon footprint reduction. Finally, by providing a driver for the EU single market in the globalised and digitised economy, Cloud computing can contribute to fulfilling the objectives of the EU2020 strategy and of the Digital Agenda flagship initiative.

However, the lack of user trust particularly in the level of security and data privacy afforded by Cloud services is often perceived as a bottleneck for the uptake of Cloud computing. While every Cloud provider has to address concerns of their customers individually, there is truly a need for the industry as a whole to take commonly recognised measures to build trust in Cloud computing.

A common set of standards covering specific, trust-critical areas in Cloud computing and a related certification regime could be a useful instrument to address cross-cutting customer concerns. However, such a standardisation and certification scheme should neither undermine the variety and scalability of current or future business models, nor try to impose unique solutions to all of them. And nor should it be limited to mere technical elements. Rather, it should seek to cover in a technology neutral manner the legal compliance issues related to Cloud computing which constitute major concerns for customers, especially in the fields of security and data privacy where both the business needs of providers and the expectations of customers must be met with certainty.

In order to fulfil that objective with sufficient accuracy and to avoid any unconstructive blanket approach that would limit the diversity in Cloud computing scenario's, the set of standards should have following characteristics:

- They should take into account the varying scale and maturity of market players & Cloud

customers targeted by the various Cloud offerings and business models.

- They should take into account the legal, contractual and operational aspects of the partnerships between the Cloud service providers that are partnering to deliver the service
- They should take into account the specific vertical industry requirements (e.g. finance, healthcare)
- They should be in line with the specific needs and market requirements associated with privacy & security that are applicable for the service considered.

a. Different Cloud customers to accommodate

Many large enterprise (LE) or large public authority (LPA) customers are already able to take advantage of the benefits of Cloud computing, either within their internal IT environment (private Cloud) or beyond, e.g. when leveraging public Cloud offerings. While often implying specific compliance requirements on them, their size also affords them a bargaining power which often allows them to negotiate tailored service level agreements with their Cloud providers, precisely so as to meet their compliance requirements. In such scenarios, certification against a common standard could be as much of a trust factor for customers as a selling point for the Cloud providers.

Small and medium enterprises (SME) and public agencies (SMPA) on the other hand often have lesser internal IT infrastructure and fewer resources. Therefore they rely more on public, or possibly hybrid Cloud service offerings. Whereas they are probably those who have the most to gain from accessing professional IT services from the Cloud on a pay-per-use basis, they also have less negotiating power or expertise than their larger counterparts, and will therefore tend to use adequately customised off-the-shelf products rather than truly bespoke services. As high Cloud adoption can allow SMEs and SMPAs to minimise their IT investments and costs, and thereby enable higher agility and increase competitiveness, respectively efficiency, it is important to assist them in taking the leap forward. In their case, a common certification scheme could be helpful in reassuring them that making the move to the Cloud will not compromise their ability to stay in control of their assets or to meet their compliance requirements, even if they choose readily available solutions rather than tailored or *sui generis* ones.

b. Different requirements to meet

While many of the benefits of Cloud computing derive from the technology's global dimension and ability to transcend the boundaries of national jurisdictions, the legal requirements, market structures and customer expectations may still differ widely in the various EU member states.

This makes the scalable provision of Cloud services less efficient and possibly more expensive in the European single market. Short of fully harmonising legal requirements and local specificities throughout the EU, a commonly shared and mutually recognised set of standard and certification schemes to cater for the different business models, particularly on the outstanding issues of security and privacy, could be helpful in mitigating this kind of fragmentation, and therefore allow Europe to better leverage the benefits of the Cloud while maintaining existing regulatory compliance levels, the case being against national or sectoral requirements (e.g. finance, healthcare).

Cloud service certifications, that approve the conformity with given European, National or sectoral legal and compliance requirements that apply for the customers themselves, are most valuable in customer purchasing phases.

The Cloud certification should also take into account the contractual partner agreements between those Cloud service providers, who are contributing along the value chain of the particular Cloud service. Also the capability to provide what has been committed in those partner agreements needs to be reviewed, as customers may not get knowledge about these partnerships (SLA/QoS).

3. Existing initiatives

The most common certification standards sought today in Cloud procurement are ISO 27001 (Information Security Management Systems) and ISAE3402 (former SAS 70, business controls). These certification standards are mainly focused on information security and business controls, and are broadly known and highly accepted in their fields. Even though they are not Cloud specific¹, they are applicable to (larger) Cloud service providers and could be refined further to enhance globally recognised standards.

Cloud specific, but relatively new and not very common so far are the CSA A6 (Cloud Security Alliance, Cloud Security) and the EuroCloud Star Audit (EuroCloud, Compliance, Data Security, Cloud Operations)

They may not necessarily provide satisfactory answers to certain Cloud customers who need to match the audit statements/results derived from such certifications with the individual national or sectoral regulatory requirements they are subjected to. In particular SMEs and SMPAs may lack the necessary background knowledge and technical expertise to make that kind of assessment. As a result, they may be held back from using Cloud services more by uncertainty and doubt than by an actual risk of non-compliance. A common Cloud-specific standard, answering these customer concerns by building on existing initiatives rather than seeking to replace them, could certainly help in bridging that gap.

4. Key features expected from a common standard and certification scheme

a. Voluntary

Compliance with any standard, and certification against it, should be left for Cloud providers to seek on a voluntary basis. In that sense, certification should be conceived as an added value business proposition, and not as a market entry barrier. Only in exceptional circumstances should certification be made a mandatory requirement. This should be limited to cases where the risk assessment of the service in question justifies that certification against a standard to be the baseline requirement (e.g. where government information above a certain classification level are involved).

b. Flexible

¹ ISO is working to extend the ISO 27001 to the field of Cloud computing. This /extension however is expected to take several years.

Cloud business models as well as possible use cases are already very varied and are likely to become more diverse and more complex as mobility, virtualisation, digital literacy and broadband connectivity are all expected to increase. Therefore, the standard and related certification scheme need to be principle-based and flexible so that they can apply to any novel technology that may arise going forward.

c. Technology and vendor neutral

Cloud computing is a growing market and a currently unparalleled opportunity for European competitiveness and innovation in the global marketplace. This potential should not be stifled by mandating specific technologies or predefined solutions, which could address neither security, nor privacy in a time-proof manner given the current pace of technological evolution.

Therefore a set of standards and associated certification should be process-oriented and technology neutral, i.e. focus on the steps taken and on the effective level of compliance achieved rather than on the particular solutions used. Moreover, vendor neutrality is equally important to prevent any competitive interference in the market, so that the standard neither induces vendor lock-in situations, nor creates weakest links or single points of failure in Cloud supply chains.

d. Industry-driven

Cloud users and providers are the best placed to identify their business needs and compliance requirements both on the local and on the international level. They should therefore lead the standardisation work in the way that is best suited to meet their respective expectations. It is not necessary at this stage to call on formal standardisation bodies to duplicate work that can be done more pragmatically by the market players themselves.

That being said, it is nevertheless important to earn the support and endorsement of those public authorities and regulatory agencies that are in charge of enforcing the particular compliance requirements which the standard is meant to address, in particular in the fields of security and privacy. Therefore, these public authorities should be associated to the standardisation efforts, to ensure consistency between the requirements of the industry standard on the one hand, and the applicable legal provisions on the other (e.g. technical and organisational measures required to protect personal data).

e. Comprehensive

As the key issues that standards are expected to address relate to the compliance requirements that customers have to meet when using Cloud services, it is critical to leverage existing Cloud certification schemes and internationally accepted standards and frameworks that can be helpful in this respect (i.e. the already mentioned EuroCloud Star Audit, CSA A6, ISO 27001, SAS70, etc.)

However, as already mentioned, these only address parts of the issue at hand, and additional aspects may also need to be covered. Depending on the business models and use cases considered, these could range from data privacy and related processes, to infrastructure security, or the case being scalability or interoperability.

On the particular topic of security, while there are a number of standards already dedicated to information assurance, certain specific points may deserve closer attention, such as, at least for certain categories of services, rules on electronic identification of both Cloud providers and Cloud users, rules applicable to related certification authorities and public key infrastructures, as well as resilience requirements (security, continuity and recovery) on infrastructures and services for example related to certain critical missions or functions, particularly of public authorities and operators of public services (e.g. e-government and g-Cloud services, public eID architectures, etc). To the extent that such requirements are already – or may at some point become – enshrined in regulatory requirements, it is important to ensure that the certification mechanism also extends to assuring compliance in these areas as well.

f. Mutually recognised across Europe

In line with the technology and vendor neutrality expected from the scheme, certification schemes should be carried out by independent organisations to be set up and/or designated with a view to ensuring that:

- The certification is carried out per Cloud service offered on the market and across all involved partnering Cloud service providers, who are delivering contributory services
- The certification remains affordable so as not to bar small and medium Cloud providers from accessing it (in particular, it is recommended to ensure a one-stop-shop process for certification);
- A certificate delivered by any designated certification authority is fully recognised and accepted across the single market not only by market operators, but also by public authorities, including in the framework of public procurement if/where relevant.

5. How to proceed

- **Short Term**

Identify the real expectations of Cloud users and authorities as well as the actual business needs of Cloud providers, particularly in the fields of security and privacy, that could be best addressed through standardisation and related certification mechanisms (as opposed to other means); define the cases in which – and thresholds above which – such certification may be desirable.

By relying to the extent feasible on existing industry platforms, and with the support of the European Commission and relevant public authorities, stakeholders should convene and define the core elements of such a standard.

- **Mid Term**

Build on existing IT certification regimes to undertake the creation of a voluntary, industry-led, technology and vendor neutral standard and related certification mechanism(s) to address the identified needs and specificities of Cloud services; this objective should be pursued at the largest possible scale (at least pan-European) , while catering for mutual recognition of certifications across regions, as well as within Europe in so far as needed to prevent that the internal market becomes fragmented between diverging national schemes and requirements.

6. Who to involve

- Members of the Trust, Security and Certification working group
- Other relevant Cloud providers and users (business users only)
- Industry organisations pursuing similar or complementary objectives (e.g. EuroCloud, CSA, ISO)
- To the extent necessary, European and national standardisation bodies already covering certain aspects to be addressed in the standard
- ENISA as well as national network and information security agencies in the EU
- Member states' data protection authorities (members of the Article 29 Working Party)
- EU and national government agencies in charge of defining Cloud strategies, whether focused on regulatory or procurement matters

Annex 7

Requirements from a Research and Innovation Point of View

(Contribution to Action Item EC/I.9B)

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

We see a rapidly growing complexity of applications deployed in Clouds, and a related growth of data and computation volumes that are handled in Clouds. This is partially due to new growth areas such as the Internet of Things or the provisioning of seamless services across multiple mobile devices. It is also due to a growing confidence of organisations which consider migrating ever increasing parts of their current in-house IT landscape into Clouds. This growth in volume is also reflected in the overall growth of the Cloud market. Growth can be expected to be exponential in the coming years, in alignment with the overall growth of data and computation on the Internet.

Singular Cloud providers are answering to this with a significant individual increase of their Cloud data centre capacity and a further push for Cloud data centre efficiency. This raises research issues such as handling big (petascale) data in the Cloud (e.g. map-reduce), Cloud management optimisation (e.g. load balancing across large compute clusters, computation near the data) and Cloud energy optimisation. Connected to this are issues of security, privacy and regulatory compliance, in particular for demanding application areas such as Healthcare.

But the use of singular Cloud providers also comes with risks, such as provider lock-in and limited resilience (e.g. due to threats such as distributed DOS attacks). Therefore, the market pushes for Clouds that are increasingly interconnected and interoperable with mechanisms such as Cloud federation, Cloud aggregation and Cloud brokerage. The resulting integration scenarios, however, raise a number of further research issues such as managing trust, risk, self-healing and legal compliance across multiple Cloud providers.

Other research issues arising from the same scenarios are: management mechanisms and open standards for Cloud federation and data-centre networking; identification, authentication and verification of persons, devices and data across complex Cloud architectures; Cloud resilience and fault tolerance in hybrid Clouds; Cloud security, privacy and regulatory compliance in hybrid Clouds; guaranteed QoS to the end-user, monitoring, auditing and SLA awareness.

Certain issues are far from being sufficiently addressed by current Cloud offerings, and they are also only partially addressed by current research. In particular the vision of a federated Cloud environment is only to a limited extent addressed by current Cloud offerings. This is also linked to the still heterogeneous adoption of open Cloud standards by the major providers. On the other hand, the vision of federated Clouds has been strongly supported by the ICT customer community – e.g. via the Open Data Center Alliance. The federated Cloud vision provides a growing market opportunity and Europe needs to further build on the early strength that it has developed in the related research domains as stated previously. The same applies to the complementary topics on the management and design of large-scale singular Clouds (with massive parallel compute cluster capacity) – a competence that few industrial players in the world currently have.

Research on Cloud computing also needs to be closely aligned with the research on large-scale applications that may be deployed in the Cloud as well as the related development of platforms. In particular it is of interest, how application, data and platform architectures can be optimised for the Cloud. Also it is of interest, how the Cloud can be optimised for specific types of services or content. This further implies issues of user experience and frontend-level technologies. The close cooperation of basic Cloud research (singular and federated) with applied areas further allows to better understanding the complex requirements of applications in the Cloud – ranging from issues such as performance and latency to regulatory compliance.

It is also necessary to find ways to involve innovative and creative SMEs which constitutes the major part of the European ICT ecosystem contributing to platform and application developments. Indeed, quite often spinoff from public or private research, they are particularly flexible and fast enough to create Cloud based services which meet customer needs or even create them. Research work should range from new concepts and features increasing ease of use and learning on any device, to open development framework for rapid prototyping and deployment.

In addition, pilot projects should be established to test innovative Cloud applications with business user in key European industries. This will allow the European alignment of Cloud infrastructure¹ research (large groups and research labs), Cloud application research (SMEs and research labs) and Cloud customers (industry).

One possible approach to this could be an EU-funded community Cloud modeled on the Japanese J-SaaS approach. J-SaaS is a community Cloud computing platform funded by the Japanese Ministry of Economy, which is designed to be an incubation platform available to SaaS providers and users. J-SaaS has been implemented under a contract with a commercial Cloud provider. This concept could be developed in Europe in a number of ways:

1. As a computing resource available in the context of a pan-European mutual aid and assistance plan for emergencies (both physical and cyber).
2. As an incubator for SME innovation. Just as government support for transport and telecommunications networks act as a catalyst to business development, so government support for such a community Cloud service, could also be an effective way to stimulate both the European Cloud industry and the innovation of new services operating on top of it.
3. As a supra national virtual space for e-government where a consistent and harmonised set of rules could be applied, both in terms of legislation and security policy and where interoperability and standardisation could be fostered.

An important factor in the success of such a venture would be to ensure that government funding does not distort the market for commercial Cloud offerings. This could be achieved by

- Focusing on e-government which would be government funded in any case.
- Selecting areas where SMEs would not otherwise be willing to try Cloud computing and by offering a try-before-you-buy model for a limited period
- Focusing on areas where public-sector intervention is a pre-requisite, such as emergency computing resource provisioning following a natural disaster.

¹ Infrastructure includes platforms, computing, storage and network resources

Research should focus on the ecosystem the Cloud evolves in, and on the challenges that it still faces. Research priorities should focus on identifying common Cloud infrastructure components and implementing them as building blocks with standard interfaces; Cloud scenarios: advance standardised and open approaches for managing Cloud resources, including computing, storage and network resources, in a coherent way; development of integrated application-aware management mechanisms able to address application-specific resource management logic; and integration of energy-aware infrastructure management and use of green IT.

Cloud research, as described previously, essentially demands pilots on Cloud infrastructure (i.e. platforms, computing, storage and network resources). In European Research & Innovation projects this is typically achieved by either temporarily setting-up a pilot Cloud infrastructure during the project runtime, or by using existing commercial Cloud services. Both solutions have deficits. Whereas the first approach allows prototyping new technologies on the infrastructure level, it typically does not sustain this environment beyond the project; the second approach is limited by the available technology and standards of commercial providers. Also both approaches demand a substantial ramp-up effort from projects. The availability of new Cloud infrastructure pilot environments will make this more flexible and efficient. This also applies to application domain specific research that would like to use a state-of-art Cloud infrastructure.

Public research funds should be targeted to three important technical aspects of Cloud Computing

- (i) Scalability of Cloud management systems: With the growing number of applications, the management tools need to grow with the size and number of systems.
- (ii) Cohesion of federated management schemes: Outside the prototypical web-startup and web-scale giants, most of the newer Cloud based applications require the collaborative management of Cloud infrastructures of several players.
- (iii) Scalability and robustness of applications and application building blocks: The distributed nature of Cloud infrastructures and the unique failure characteristics of Clouds require a rethinking of the entire software stack and development

The European Commission and Member States should create a platform to share and develop best practices for Cloud computing in the public sector. A sound public sector strategy would encompass inter alia technical and regulatory standards to address data security and privacy concerns, financial incentives and appropriate budget models to procure Cloud services, and a platform to exchange best practices. Any national public sector Cloud strategy should become an integral part of an overall public Cloud policy to advance Cloud computing in all areas of the economy and society.

Firstly, it is important to advance standardised and open approaches for managing Cloud resources, including computing, storage and network resources, in a coherent way. In that context, common Cloud infrastructure components should be identified and these should be implementable as building blocks with open standard based interfaces. Public R&I funding can support this process but it should be linked to Cloud open source or multi-vendor framework developments, such as OpenStack or OpenNebula.

Secondly, there is a need for allowing a better collaboration of infrastructure level Cloud research, which could be realised through shared Cloud R&I infrastructure that lives beyond the end of an individual project. This would also allow hosting of applications and platforms. In this regards, the Future Internet Core Platform project and the FI PPP Programme structure (including the usage area projects) points in the right direction.

Annex 8

Comprehensive Inventory of Relevant Existing and Emerging Cloud and Internet-related Standardisation and Interoperability Initiatives

(Addressing Action Items I.10A)

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

Preliminary Remarks – Objective of this report:

As Cloud Computing gains momentum, concerns are being raised by users that they will not have the ability to easily move their data and applications between different Cloud environments. Openness is a result of BOTH the use of technical standards for interoperability at all levels, AND commercial SLAs that do not unduly limit transfer of contract or impose any other unacceptable restrictions on user choice.

The first way to address these concerns, and to minimise perceived “lock-in” situations, is to ensure that Cloud Computing is based on industry recognised standards that help to promote data interoperability.

The recommendations made in the ICT Standardisation Review and included in the Draft Regulation give a positive lead and exemplar whereby not only support for fora and consortia is given, but active assessment of standards criteria will be undertaken. It is our view that within Cloud the market will increasingly deliver necessary standards through such fora/consortia alongside SDOs and the Commission can take an active role in their determination and acceptance.

Industry Vendors were requested by the EU 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 that Cloud Computing is approached in an open and global manner.

Industry Vendors were also requested to analyse the inventory jointly with all stakeholders (demand and supply including consumers) to understand what improvements, if any, can be made in terms of transparency and efficiency of the process. Recognising the strong interest of all stakeholders in interoperability for Cloud computing along with the fact that many relevant technologies exist and interoperability efforts are ongoing, this report intends to clarify where we are and where we need to go in order to meet the related needs.

The Report is structured in three parts: Current Landscape and Recommendations, which represent consensus conclusions; Part A, which is an inventory of the Cloud and Internet related standardisation and interoperability initiatives; and Part B which gives an overview of the challenges and possible areas of improvement, reflecting the variety of responses received in May 2011 from the companies

participating to the WG on Data Portability, Interoperability and Reversibility that provided input into our deliberations.¹

EXECUTIVE SUMMARY - CURRENT LANDSCAPE AND RECOMMENDATIONS

The major concerns of users include:

- Data portability: the capability for a user to take data that is placed into one Cloud computing environment and move it to a different Cloud computing environment, with minimal effort.
- Application & Service interoperability: the capability for applications and services hosted in Cloud computing environments to interoperate with one another – and for the client to have a consistent interface when using these applications and services.
- Application portability: The capability for an end user to move their application code from one Cloud computing environment to another Cloud computing environment with minimal effort.
- Ease of Migration: as well as being able to move applications and data from one Cloud computing environment to another, users have the need to be able to remove all their materials from a particular Cloud computing environment and be assured that nothing remains there. (The “right to be forgotten” as it is sometimes termed)

Overview of global industry standards relating to Cloud computing

In beginning this process, it became apparent that there are 2 classes of specifications and standards that need to be examined, since Cloud Computing is in many cases an extension of existing capabilities. These two classes include:

- general computing standards; and,
- emerging set of Cloud specific standards.

Both of these classes of specification can serve as guidance to the industry to enable the creation of open computing environments that provide interoperability and portability.

The evaluation of existing standards

This document provides an evaluation of existing activities relating to Cloud computing standards:

- Presents a categorisation to help identify existing standardisation efforts; and,
- Identifies priorities for formal standardisation activities and rationalise competing specifications to prevent market fragmentation.

The results of this exercise can be summarised as follows: there are many ongoing activities in relation to Cloud Computing specifications and standards – it has not been possible to discover detailed information about some of these activities due to access problems (*e.g.* activities with no published public material). This would require further work with the organisations concerned.

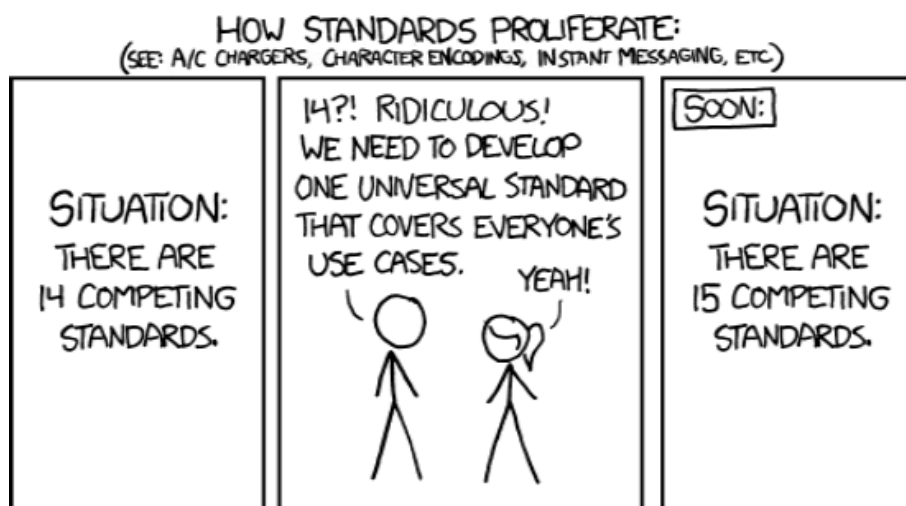
There are multiple initiatives already in process in all areas relevant to Cloud computing, either as Cloud specific initiatives or as general initiatives that cover relevant aspects of the Cloud, making it a

¹ It should be noted that the questionnaire focussed on technical aspects related to portability, interoperability and reversibility, and did not encompass ‘regulatory interoperability’, a topic which we consider should also be addressed in the future, as pointed out during the November 2011 Data Protection Commissioners Conference in Mexico.

very dynamic environment. In general, these efforts are driven by an approach whereby standards are put in place in response to defined use cases.

Our Recommendations in this area:

- a. Cloud Computing requires interoperability and portability: industry acknowledges that market-driven standards are essential and work in this area is well underway.
- b. Standards should be global (and not local/European) to support the global and scalable nature of the Cloud.
- c. Regulation of interoperability and portability is premature at this early stage of the Cloud and in light of the market-led initiatives. Ongoing monitoring of and participation in these initiatives by interested governments and user organisations are welcome and encouraged. At the same time, industry should continue to ensure that market-led initiatives are progressing to meet identified needs, and participate in efforts to demonstrate interoperable solutions even as work on relevant standards proceeds.
- d. New standards should only be created where they add real value and are aimed at solving real problems. In many cases, identified problems can be solved through the use of existing standards. In parallel, at a pragmatic level, testing procedures to evaluate interoperability should be considered, for example through voluntary certification programs.



xkcd.com/927 image reuse permitted by Randall Munroe's
creative commons attribution-noncommercial 2.5 license

- e. Our recommendation is for the EU to monitor and potentially participate in these efforts, particularly the international activities such as those taking place at in fora/consortia such as ISO and ITU-T, to make sure they provided the needed direction to industry, and to openly support those initiatives that benefit the Cloud ecosystem.
- f. The Cloud Observatory being discussed in the WG on Uptake & Innovation could play a role in this area by setting up a meeting between:
 - Commission and member states experts; and
 - EU industry experts active in standardisation bodies to enhance the flow of information and evaluate on a regular basis the advancement of the various roadmaps
- g. A key issue is ensuring that where there are specific issues arising from interoperability within the public sector operations – be it in member states, between member states and

between member states and other European organisations – that these are properly understood and put forward as requirements to the relevant standards bodies. A commission led exercise collating such requirements and use cases would be a significant step forward in ensuring public sector requirements are addressed that may otherwise not be brought forward to technical standards committees. At the same time this would highlight public sector demand, ensure that public sector requirements are met by the market and prevent unnecessary fragmentation of standards between sectors.

PART A – INVENTORY OF CLOUD AND INTERNET RELATED STANDARDISATION & INTEROPERABILITY INITIATIVES

I. Definition of Standards and Scope of ‘Cloud Relevant Standards’

Within the context of the ICT Standardisation Review and Draft Regulation reference is given to WTO criteria in selection of a standard and specification, as well as to the referencing of fora and consortia. Annex II of COM(2011)315/2 makes specific recommendations on “Requirements for the Recognition of Technical Specifications in the Field of ICT” which cover such areas as market acceptance, tests on the openness of the developing organisation, and on the availability and usage of that specification in the market.

Within the area of software interoperability (which covers the majority of Cloud standards) the European Interoperability Framework (EIF) has provided additional and more specific recommendations in the formation of an applicable open standard. The EIF is particularly relevant in its intention to encourage harmonisation for pan European interoperability. To quote “*The EIF should be taken into account when making decisions on European public services that support the implementation of EU policy initiatives. The EIF should also be considered when establishing public services that in the future may be reused as part of European public services*”.

The ‘definition’ used in the EIF sets out the following process:

“If the openness principle is applied in full:

All stakeholders have the same possibility of contributing to the development of the specification and public review is part of the decision-making process;

The specification is available for everybody to study;

Intellectual property rights related to the specification are licensed on FRAND terms or on a royalty-free basis in a way that allows implementation in both proprietary and open source software”.

Cloud computing is an evolution of many existing technologies so by nature, it is built on and adheres to general computing standards already in practice. On top of these general standards, additional ‘Cloud-specific’ standards are emerging to help guide the maturation of Cloud in ways that allow users to have necessary interoperability, portability, data protection that will allow them to the freedom to move between different Cloud environments.

In most cases the general standards are well-established and have well-defined paths for evolving the standards while the Cloud specific specifications and standards are still under development with initiatives being established as the need becomes recognised. This implies that any important use cases are addressed in a timely way (see for example the proposal for a new Working Group on data protection and privacy issues within ISO WG SC 27 issued put forward in mid-2011 and which covers some of the use cases not yet addressed elsewhere, from the perspective of data handling practices and controls).

In order to avoid replication of work and minimise market fragmentation many of the mature general standards are likely to be adopted by ISO/IEC rather than new standards being created at national or EU levels. This will be complementary to the processes expected following the adoption of COM(2011)315/2.

Ensuring that data can be imported and exported into different Internet services in an open, interoperable format is important in ensuring Cloud specific standardisation efforts meet user demand.

The best practice approach taken by companies so far has been that Internet standard formats have been used wherever possible, and where standard formats do not yet exist, formats used are openly documented.

II. Categorisation of Standards

In creating the list of specifications and standards, we have identified 11 areas to which standards and specifications can apply, and also specified if, in the case of Cloud specific standards, they apply to IaaS, PaaS or SaaS types of Cloud service, or to all of them.

It is important to note that in some cases, no Cloud specific standards are developed in a certain category, as that category covers an area which is much broader than the Cloud. A typical illustration is the Transport Category. Standards also apply to specific types of Cloud services depending on their relevance to the service provided. This is the case for example with Infrastructure API's, which are only relevant to the IaaS type of Cloud services.

Note that some of the initiatives listed in the Annex have not been integrated in our categorisation effort below, as it was not possible to receive sufficient information on the activities of the concerned body.

The 11 areas used to categorise the standards work cover different sets of capability which reflect various aspects of the use of Cloud computing environments by users, all of them necessary to achieve the overall goals of interoperability and portability.

- Identity – capabilities relating to the identity of a user
- Platform APIs – client programming interfaces relating to a Cloud computing platform
- Infrastructure APIs – client programming interfaces related to the setup and management of Cloud infrastructure
- Data APIs – client programming interfaces related to the management of storage and data in the Cloud
- Data Privacy - specifications dealing with data protection and data privacy
- Security – specifications dealing with security related capabilities including encryption, authentication, authorisation.
- Environment – capabilities relating to the wider environment of a Cloud Computing platform such as Audit capabilities
- Quality of Service – capabilities relating to Quality Of Service aspects of a Cloud Computing environment
- Management & Monitoring – the management and monitoring of a Cloud computing environment
- Transport – capabilities relating to how data is moved to/from a Cloud computing environment
- Other areas – anything which cannot be placed into one of the above categories

We refer you for more details to the Appendixes to this Report: Appendix A matches, where feasible, the identified standardisation initiatives per category and their scope of application; and Appendix B gives more background information on the various standards and specifications bodies considered in the analysis.

PART B - OVERVIEW OF CHALLENGES AND POSSIBLE AREAS OF IMPROVEMENT

I. The need for interoperability: striking a balance between standardisation & innovation



Standardisation is key to the widespread adoption of Cloud services in Europe and globally: only an open and interoperable Cloud environment can provide to end users the full benefits of the Cloud. End users want the freedom to choose services from various Cloud providers without getting locked into infrastructures that prevent the seamless migration of data and services. However, this standardisation needs to be implemented in a way that allows vendor innovation and the continued maturation of the Cloud.

The Working Draft of the HTML 5 proposed standard document provides a good summary of a best practice approach to standardisation and resulting interoperability by stating: *“this specification is intended to define an openly-produced, vendor-neutral language, to be implemented in a broad range of competing products, across a wide range of platforms and devices”*.

II. The different layers of interoperability and portability

The ‘Cloud’ is not a monolithic concept, as there are different types of Clouds providing different capabilities catering to the needs of different types of users.

It is therefore necessary to understand the needs of the different customers in the different segments. The requirement and standardisation in the context of a large enterprise (more than 500 employees) may be different to a small enterprise (max. 20 employees) or even to individual users. Standardisation should hence be encouraged based on the requirements of the different customer segments to obtain long term benefits.

It is also important to recognise that “Cloud Computing” covers a wide range of capabilities, from the provision of basic computing capability (“IaaS”) through the use of platforms able to run specific kinds of application (“PaaS”), to the direct provision of complete services (“SaaS”). These differing capabilities have differing specifications and different standardisation needs.

Moreover, it is important to note that there are different kinds of “interoperability” and “portability” at play in the Cloud environment, with different potential levels of attainment:

- Data portability: the capability for a user to take data that is placed into one Cloud computing environment and move it to a different Cloud computing environment, with minimal effort.
- Application & Service interoperability: the capability for applications and services hosted in Cloud computing environments to interoperate with one another - and for the client to have a consistent interface when using these applications and services.
- Application portability: The capability for an end user to move their application code from one Cloud computing environment to another Cloud computing environment with minimal effort.

- **Ease of Migration:** as well as being able to move applications and data from one Cloud computing environment to another, users have the need to be able to remove all their materials from a particular Cloud computing environment and be assured that nothing remains there. (The "right to be forgotten" as it is sometimes termed)

The focus should realistically be to ensure that there are no artificial barriers that prevent interoperability and portability.

Finally, different aspects of Cloud computing are at different stages of maturity, and standardisation should consider current adoption and maturity as well as continuing evolution in different aspects and in relation to specific use cases. The speed at which the market evolves makes it more difficult to set up well defined standards before the market consolidates. All the process of establishing standards should be done with great care, to avoid the risk of reducing the pace of innovations introduced by the industry.

At this point in time, the technology at the infrastructure layer is relatively mature and standardisation should be encouraged. In fact, even without encouragement, numerous components have already been standardised, and several other standardisation initiatives are currently underway. These efforts should be generally supported, but caution should be taken to ensure that competing standards don't arise.

As one moves up the technology stack, however, in general the level of maturity decreases and the level of innovation increases. For that reason, standardisation at these layers should be done with care and only once requirements are clearly understood. In no case, and at no level of the technology stack should standardisation be imposed through regulation or other means.

III. State of play and identification of certain interesting initiatives relating to Cloud Computing.



As set out in our report on standardisation, work is in progress in various fora such as IEEE, DMTF, ISO, SNIA, SIENA, Open Group, OpenStack, etc. These and other activities will continue to progress. Since Cloud Computing is the delivery of applications, data, and services using established Internet technology, most of the underlying standards of the Internet apply to the Cloud.

Because of the extent of the hardware/software stack that make up Cloud computing, it is necessary to explore interoperability and resulting standards on all level. This ranges from the hardware (server, storage, networking) infrastructure, operating system and/or hypervisor level, APIs and related development standards, and formats used to store/retrieve data.

There are various efforts which aim to provide roadmaps of the standards relevant to Cloud Computing. These include the work being done at NIST in the USA and work being done in some of the standards bodies such as ISO. There is also a standards roadmap effort in the SIENA Initiative - which is EC funded and publically referenced by Vice President Kroes. The European Commission should strongly encourage participation to make SIENA properly representative of pan European needs, while at the same time ensuring that SIENA is linked strongly to the wider international efforts.

Moreover, Digital Agenda actions will address many needs, and the EC can create regular process to monitor industry action and progress, expose gaps, stimulate/support industry-led global standardisation, raise awareness of existing efforts and possibilities, sponsor/fund the demonstrators and plug fests and other practical efforts to make interoperability a reality. The EC is funding some FP7 Cloud projects that have an emphasis on interoperability, and active reporting of results would be useful.

Also, governments must enforce procurement processes that are public and open and in which establishing requirements of interoperability can encourage the design and implementation of interoperable Clouds.

Public procurement processes may need to be adapted, since they may be poorly-suited to leasing software as a service rather than purchasing software as a good. There is typically a change in balance between up-front costs and ongoing costs. There may also be a requirement for pilot programmes to demonstrate capabilities, including appropriate security and privacy protection. Clear leadership will be needed to handle these changes in a public sector context.

Establishing processes for providing financial incentives and rewards for agencies as they take steps towards implementing Cloud deployments could be another way to improve adoption (possible approaches could include allowing agencies to retain and redirect a portion of budget savings). From an administrative point a view, public-procurement processes should be open and transparent, and should require that all bidders provide a clear path for standards-based interoperability and to provide for data portability so that the public agencies are not locked in to any particular technology or vendor. Finally, by making the procurement process simpler, faster and cheaper, the Member States Governments could open up the market to new players and remove two of the biggest barriers for new entrants, which are the cost and length of the procurement process.

V. Minimum Requirements and Possible Areas of Improvement



The lack of fully-fledged interoperability and portability is a quite typical symptom of early stages of markets and, in a way a necessary phase when testing out different innovative approaches, and where convergence will happen over time, as the “best” approaches become manifest – and over time, interoperability and portability will be in the natural self-interest of market players because it creates a bigger market for everyone and is the way to meet consumer demand.

Current standards may not have all the flexibility to support well enough interoperability and portability between different Clouds and especially between Clouds in different member states of the EU. If we want to also create mobility of Cloud services and also advanced features such as load balancing between Clouds, we need to consider some additional functionalities. Well managed interfaces and data formats are necessary to enable communications and data exchange between different Clouds, while a key end user demand is portability of data (data constructs like identity, events and others related to data).

Data portability is best ensured through the use of open standards and open interfaces. The concept of data portability, however, should not be interpreted to imply that portability of all features and functions. Product and service differentiation are part of increased market choices and help drive effective competition between providers.

The Cloud is not a unitary offering and no one-size-fits-all solution can be crafted. Furthermore principles of interoperability and focusing on the role of open standards are more important elements at this time than any top-down imposition of requirements.

More specifically, there is a need to use the term “interoperability” with care, since in the Cloud space, it can apply to a range of different things.

So, for example, where an application is deployed to one Cloud platform, it should be able to interoperate with applications deployed to other Cloud platforms using standard interoperable protocols such as Web services. On the other hand, when considering the programming interfaces or user interfaces that the customer of a Cloud computing platform may use to deploy and control applications, then there may not today be any agreed standards that apply to different Cloud platforms. However, any new standards in these areas need to be market led and internationally agreed.

We would also like to stress that the notion of “national Clouds” or even a “European Cloud” should be looked at in a global context. It should certainly not result in a set of specific requirements (functional requirements, standards, legacy requirements, etc.) that would differ significantly across countries and hence would complicate the EU Single Market (and complicate the life of companies that operate across borders). If the EU initiative will include direct commentary on such Cloud initiatives, the strategic direction should be to consolidate and streamline various EU Member State initiatives and requests and feed them into the global standards discussion.

From a policy perspective, we support Commissioner Kroes’ statement that the EU should play a stronger role in the technical standardisation of Application Programming Interfaces (APIs) and data formats to enhance interoperability and competition between Cloud providers, as long as this is done in the context of global international standardisation. Moreover, the Digital Agenda pillar on interoperability is comprehensive approach encompassing a range of actions (improvements to the standardisation system, stimulate use of standards esp. through public procurement, stimulate licensing of interoperability information for non-standardised technologies, implement the EIF...). These actions are relevant to all ICT, including Cloud computing.

The concern about data control and portability has some added emphasis in the Cloud context, and maybe EU strategy should be based on the foundation that clients own their data and that Cloud platforms should make it easy and efficient to securely move customers’ data in and out.

In more detail, we believe that:

1. Open standards and protocols are absolutely fundamental. APIs are a first possible solution but not enough. APIs that allow user programs running in the Cloud to export data in standard format(s) are needed.
2. Standard testing for interoperability should be considered (certification programs)
3. A stretch goal is to be able to run applications in more than one Cloud at once and allow for direct interaction among the Clouds.
4. At minimum, data and programs need to be movable between Clouds although some Clouds may not allow arbitrary user code to run.
5. "The right to be forgotten" is required - ie the principle that a customer of a Cloud environment should be able to remove all their data and programs from that environment and be assured that nothing of theirs has been retained by the environment vendor

The Cloud Observatory being discussed in the WG on Uptake & Innovation could play a role in this area by setting up a meeting between:

- Commission and member states experts; and
- EU industry experts active in standardisation bodies to enhance the flow of information and evaluate on a regular basis the advancement of the various roadmaps.

Appendix A: Detailed inventory of standards and their scope of application

A. Identity

Cloud specific standards

OASIS	Identity in the Cloud	Applies to all types of Cloud
-------	-----------------------	-------------------------------

General standards and specifications relevant to Cloud computing

IETF	OAuth	Applies to all types of Cloud
Open ID community	Open ID Authentication	Applies to all types of Cloud

B. Platform API's

Cloud specific standards

Apache	Nuvm	Applies to PaaS
--------	------	-----------------

General standards and specifications relevant to Cloud computing

None identified.

C. Infrastructure API's

Cloud specific standards

DMTF	OVF	Applies to IaaS
Apache	LibCloud	Applies to IaaS
Apache	DeltaCloud	Applies to IaaS
OpenStack	Image Service	Applies to IaaS
OpenStack	Compute	Applies to IaaS

General standards and specifications relevant to Cloud computing

None identified.

D. Data API's

Cloud specific standards

SNIA	CDMI	Applies to IaaS and Paas
OpenStack	Object Storage	Applies to IaaS

General standards and specifications relevant to Cloud computing

None identified.

E. Data privacy

Cloud specific standards

ISO WG SC27	Data Privacy (to be adopted)	Applies to all types of Cloud
-------------	------------------------------	-------------------------------

General standards and specifications relevant to Cloud computing

OASIS	OASIS Privacy Management Reference Model	Applies to all types of Cloud
-------	---	-------------------------------

F. Security

Cloud specific standards

CSA	Cloud Controls Matrix	Applies to all types of Cloud
ISO SC27	ISO 27001	Applies to all types of Cloud
ISO SC27	ISO 27002	Applies to all types of Cloud

General standards and specifications relevant to Cloud computing

W3C	XML Digital Signature	Applies to all types of Cloud
W3C	XML Encryption	Applies to all types of Cloud
IETF	X.509 Certificates and PKI	Applies to all types of Cloud
OASIS	KMIP	Applies to all types of Cloud
OASIS	XACML	Applies to all types of Cloud
OASIS	SAML	Applies to all types of Cloud
OASIS	WS-Security	Applies to all types of Cloud
OASIS	WS-Reliable Messaging	Applies to all types of Cloud
WS-I	Web Services Security Profiles	Applies to all types of Cloud
ISO / IEC 18028	IT Network security	
ISO / IEC TR 18044	Information security incident management	
ISO / IEC 18043	Operation of intrusion detection systems (IDS)	
ISO / IEC 15816	Security information objects for access control	
ISO / IEC 24762	Security Techniques – Guidelines for information and communications technology disaster recovery services	

G. Environment

Cloud specific standards

CSA	Cloud Trust Protocol	Applies to all types of Cloud
CSA	Cloud Audit	Applies to all types of Cloud

General standards and specifications relevant to Cloud computing

None identified.

H. Quality of service

Cloud specific standards

DMTF	OVF	Applies to IaaS
------	-----	-----------------

General standards and specifications relevant to Cloud computing

None identified.

I. Management & Monitoring

Cloud specific standards

OGF	OCCI Core	Applies to all types of Cloud
OGF	OCCI Infrastructure	Applies to IaaS
OGF	OCCI Restful HTTP Rendering	Applies to all types of Cloud
DMTF	Cloud Management WG	Applies to IaaS
DMTF	Cloud Auditing Data Federation WG	Applies to IaaS (+ others?)
ISO JTC1 SC7	ISO/IEC 19770-3, Information technology	Applies to IaaS, PaaS

-- Software asset management

General standards and specifications relevant to Cloud computing

DMTF	WS-Management	Applies to all types of Cloud
------	---------------	-------------------------------

J. Transport

Cloud specific standards

No Cloud specific initiatives exist, as Transport is an issue that goes well beyond the Cloud and encompasses the broader Internet and telecoms worlds.

General standards and specifications relevant to Cloud computing

IETF	TCP/IP	Applies to all types of Cloud
IETF	HTTP / HTTPS	Applies to all types of Cloud
IETF	FTP	Applies to all types of Cloud
W3C	SOAP	Applies to all types of Cloud
W3C	WSDL	Applies to all types of Cloud
W3C	WS-Addressing	Applies to all types of Cloud
W3C	WS-Transfer	Applies to all types of Cloud
n/a	REST	Applies to all types of Cloud
n/a	JSON	Applies to all types of Cloud
WS-I	Web Services Profiles	Applies to all types of Cloud
OGF	GridFTP	Applies to all types of Cloud
OASIS	WS-Policy	Applies to all types of Cloud

K. Other areas

Cloud specific standards

Open Group	Cloud Computing Reference Architecture	Applies to all types of Cloud
ISO JTC1 SC38	Cloud Computing Reference Architecture	Applies to all types of Cloud
IEEE	P2302 Standard for InterCloud Interoperability and Federation (SIIF)	Applies to all types of Cloud
IEEE	P2301 Draft Guide for Cloud Portability and Interoperability Profiles (CPIP)	Applies to all types of Cloud
CIF	Cloud Industry Forum Code of Practice	Applies to all types of Cloud

General standards and specifications relevant to Cloud computing

None identified.

Appendix B : List of Cloud Computing Standards and Standards and Specifications Bodies Considered in the Analysis

This appendix gives a more detailed overview of the standards and specifications examined as part of the study, classified in alphabetical order. This list represents what we could identify ‘to the best of our knowledge’, as not all initiatives are equally transparent.

Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, Germany)

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile

The Federal Office for Information Security in Germany published in June 2011 recommendation for Cloud-Computing providers and users with special security requirements, i.e. public authorities. These recommendations are published after a consultation of different stakeholders in Germany.

CCF (Cloud Computing Forum in Korea)

CCF is a Korean organisation established in December 2009 to develop Cloud standards and promote their application to public organisations.

It is unclear what standards are being defined

CESI (China Electronics Standardisation Institute)

<http://www.cesi.ac.cn/>

Cloud Computing Standardisation Study

Operation Requirements for Cloud Computing services

Cloud Computing Interoperability Forum

<http://www.Cloudforum.org/>

Unified Cloud Interface Project - It is unclear if this WG is still active.

Cloud Computing Use Case Discussion Group

<http://www.Cloudbook.net/directories/Cloud-groups/Cloud-computing-use-cases-discussion-group>

Cloud Industry Forum (CIF)

<http://www.Cloudindustryforum.org/>

Cloud Industry Forum Code of Practice

Cloud Security Alliance (CSA)

<https://Cloudsecurityalliance.org/>

The Cloud Security Alliance was created to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.

Cloud Trust Protocol

Cloud Audit

Cloud Controls Matrix

Cloud Standards Customer Council

<http://www.Cloudstandardscustomercouncil.org/>

Not a standards organisation, but a grouping of Cloud computing users who aim to provide input on use cases and requirements for standards to relevant SDOs.

Cloud Computing Use cases whitepaper

Practical Guide to Cloud Computing

Distributed Management Task Force (DMTF)

<http://www.dmtf.org/>

DMTF is a global industry organisation leading the development, adoption and promotion of management standards and interoperable systems management. It is comprised of more than 160 member companies and alliance partners, representing 43 countries around the world.

Open Virtualisation Format (OVF) (now also an ISO standard)

Cloud Management WG

Cloud Auditing Data Federation WG

European Network and Information Security Agency (ENISA)

Though work seems to be done on Cloud relevant issues, it is unclear what standards are being defined.

ETSI Technical Committee (TC) CLOUD

<http://www.etsi.org/WebSite/Technologies/GRID.aspx>

The stated goal of ETSI TC CLOUD (previously TC GRID) is to address issues associated with the convergence between IT (Information Technology) and Telecommunications. The focus is on scenarios where connectivity goes beyond the local network.

Unclear what is being produced.

Institute of Electrical and Electronic Engineers (IEEE)

<http://www.ieee.org/index.html>

IEEE formed the Cloud Computing Standards Study Group (CCSSG) in March 2010.

Work in progress:

P2301 Guide for Cloud Portability and Interoperability Profiles

P2302 Standard for InterCloud Interoperability and Federation (SIIF)

ISO/IEC JTC 1/SC 7

<http://www.jtc1-sc7.org/>

ISO/IEC JTC1 established a Study Group to study Cloud computing. The Study Group is classifying Cloud computing, sorting out terminology, and maintaining liaison with other organisations.

ISO/IEC 19770-3, Information technology – Software asset management

ISO/IEC JTC 1/SC 27

http://www.iso.org/iso/iso_technical_committee.html?commid=45306

SC27 is studying requirements for Information Security Management Systems (ISMSs).

New Work Item proposed to extend existing Security standards to Cloud

ISO 27001

ISO 27002

ISO 29100

ISO/IEC JTC 1/SC 38

http://www.iso.org/iso/jtc1_sc38_home

SC38 has the responsibility for standardisation for interoperable Distributed Application Platforms and Services including:

- Web Services
- Service Oriented Architecture (SOA)
- Cloud Computing

Particular work on Cloud computing is:

Cloud Computing Terminology

Cloud Computing Reference Architecture

ITU-T Focus Group on Cloud Computing

<http://www.itu.int/en/ITU-T/focusgroups/Cloud/Pages/default.aspx>

In February 2010, ITU-T launched the Focus Group on Cloud Computing, which is discussing the benefits of Clouds and target issues requiring standardisation from the telecommunication perspective.

WA 1-1 Cloud Definition, Ecosystem & Taxonomy

WA 1-2 Uses cases Requirements & Architecture

WA 1-3 Cloud security

WA 1-4 Infrastructure & Network enabled Cloud

WA 1-5 Cloud Services & Resource Management, Platforms and Middleware

WA 1-6 Cloud computing benefits & first Requirements from ICT perspectives

...no actual standards being worked on at present...

KCSA (Korea Cloud Service Association)

It is unclear what standards are being defined

NIST

<http://www.nist.gov>

<http://collaborate.nist.gov/twiki-Cloud-computing/bin/view/CloudComputing/>

NIST's role in Cloud computing is to promote the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards.

OASIS

<http://www.oasis-open.org/standards>

OASIS drives the development, convergence and adoption of open standards for the global information society. The source of many of the foundational standards in use today, OASIS sees Cloud Computing as a natural extension of SOA and network management models.

Identity in the Cloud

(many other non-Cloud standards can apply to Cloud)

Object Management Group (OMG)

<http://www.omg.org/>

OMG's focus is always on modelling, and the first specific Cloud-related specification efforts have only just begun, focusing on modelling deployment of applications & services on Clouds for portability, interoperability & reuse.

Cloud Standards Customer Council

Nothing Cloud specific being produced at present

Open Data Center Alliance

<http://www.opendatacenteralliance.org/>

An independent organisation which aims to give data centre managers a voice in shaping Cloud computing requirements and solutions.

Usage Model Publications

Open Grid Forum (OGF)

<http://www.gridforum.org/>

Open Grid Forum (OGF) is a leading standards development organisation operating in the areas of grid, Cloud and related forms of advanced distributed computing. The OGF community pursues these topics through an open process for development, creation and promotion of relevant specifications and use cases.

OCCI – Core / Infrastructure / Restful-HTTP

Project group “Interoperability and Portability of Cloud Computing” of Working Group 2, National ICT-Summit, Germany

<http://www.bmwi.de/BMWi/Navigation/Technologie-und-Innovation/Digitale-Welt/IKT-Strategie-Nationaler-IT-Gipfel/it-gipfel.did=364068.html>

Work in progress. At this stage, the project group is identifying different relevant standards for Cloud-based services. In December 2011 the Project group intends to publish a guide about interoperability and standards for Cloud-computing.

SIENA

<http://www.sienainitiative.eu/StaticPage/About.aspx>

SIENA (the Standards and Interoperability for eInfrastructure Implementation Initiative) is a Support Action funded by the European Commission under Framework Programme 7 Research infrastructures projects. Running from 2010 to 2012, SIENA is trying to define a future eInfrastructures roadmap focusing on interoperability and standards.

SIENA has published the initial SIENA European Roadmap on Grid and Cloud Standards for e-Science and Beyond.

Storage Networking Industry Association (SNIA)

<http://www.snia.org/>

The SNIA has created the Cloud Storage Technical Work Group for the purpose of developing SNIA Architecture related to system implementations of Cloud Storage technology.

Cloud Data Management Interface (CDMI)

Study Group on Smart Cloud (Japan)

Smart Cloud Study Group Report

It is unclear what standards are being defined

The Open Group

<http://www.opengroup.org/>

The Cloud Work Group in the Open Group exists to create a common understanding among buyers and suppliers of how enterprises of all sizes and scales of operation can include Cloud Computing technology in a safe and secure way in their architectures to realise its significant cost, scalability and agility benefits.

Cloud Computing Reference Architecture

W3C

Nothing Cloud specific to our knowledge.

Open Source Activities

While not being formal specification or standards activity, Open Source groups are often pioneers in developing functionality for new areas of computing as well as adapting existing technology for new interoperable uses. It is not uncommon for their activities to form the basis of later specifications and standards.

- Apache LibCloud
- Apache DeltaCloud
- Apache Nuvem
- OpenNebula

- OpenStack
- Simple Cloud API