EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

Net Futures
Software and Services, Cloud

Brussels, 15.07.2014

TRUSTED CLOUD EUROPE SURVEY

Assessment of Survey Responses

1. EXECUTIVE SUMMARY

In March 2014, the European Cloud Partnership (ECP) Steering Board published their vision document, called Trusted Cloud Europe.

A survey on the Trusted Cloud Europe (TCE) report was launched on 21 March and ended on 2 May 2014. This report summarises the responses received in the survey to the key ideas on how cloud services can contribute towards a growing, sustainable digital economy.

This survey was intended to gauge the overall reactions to the issues highlighted in the report. Potential future Commission proposals concerning the relevant areas will have to be preceded by a more specific formal consultation.

2. CONTEXT

In September 2012, the European Commission adopted a strategy for "Unleashing the Potential of Cloud Computing in Europe" which is available at https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

The strategy includes three key actions:

- cutting through the jungle of Standards
- developing safe and fair contract Terms and Conditions
- establishing European Cloud Partnership

The European Cloud Partnership Steering Board was set up as an advisory body to the Commission. The board's task is to help bring together the public and private sector to advance the development of the cloud computing market in Europe.

In March 2014, the Board published its set of ideas in the form of a report entitled 'Trusted Cloud Europe' which is also available at https://ec.europa.eu/digital-agenda/en/european-cloud-partnership

'Trusted Cloud Europe' can be described as a framework for supporting the definition of common cloud computing best practices, linking them to use cases with a view of applying them in practice.

'Trusted Cloud Europe' aims at supporting the development of a single digital market for cloud computing in Europe, based on best practices and on a common understanding of these best practices.

There are two main groups of actions from the set of ideas in 'Trusted Cloud Europe': Best Practice, and Consensus Building.

The 'Trusted Cloud Europe' report has been the subject of an online survey.

3. PROCESS

The survey took the form of an online community and questionnaire. The community included discussion topics curated from 'Trusted Cloud Europe'. People were invited to comment freely on those topics. People could also respond by email.

The questionnaire consisted of structured questions with multiple-choice answers. This focussed on very specific issues of importance within 'Trusted Cloud Europe'. (The questionnaire is available in the Annex)

The topics for the community and the questions & answers in the questionnaire included questions surrounding cloud-active policy, procurement rules, geographical restrictions, and digital single market. (More detail of these survey topics is also available in the Annex).

Three criteria were used to assess the response:

(1) agreement (percentage of 'AGREE' responses to questionnaire),

(2) impact (qualitative assessment of email responses),

(3) focus (due to the volume of questionnaire responses and manner in which they were collected, this is a percentage of comments from email and online community responses only. These comments were linked to topics in the questionnaire for this assessment).

While a more detailed analysis of the responses can be found in the Annex, the main observations from the respondents are summarised below.

4. RESULTS

The survey on the TCE document ran for 6 weeks from 21 March to 2 May 2014 and received 283 responses in total (online community discussion comments: 6, Email responses: 25, Questionnaire: 252). This exploratory survey was designed to collect and examine initial responses to the TCE proposals. The feedback may be used to fine-tune any future Commission initiatives or further consultations on cloud computing. A more specific formal consultation will be necessary before any Commission proposals are put forward.

The survey results indicate support for the key ideas suggested by the ECP Steering Board as follows:

(1) encourage information security that is balanced with consumer and provider needs (93% agreement),

(2) support application of the data protection and data privacy framework with particular relevance for cloud computing and harmonisation of the framework across Europe (82% agreement),

(3) provide clearer rules to resolve contractual or service level agreement disputes (79% agreement),

(4) establish recognition of a Trusted Cloud Europe brand to build user trust (76% agreement),

(5) support standards and certification without inhibiting innovation (73% agreement),

(6) review data categorisation and impact of existing legislation, in order to identify formal (such as legal and technological) requirements, including data location requirements, and identify possible functional requirements that could serve as acceptable substitutes in order to further develop Trusted Data Flow within the Digital Single Market for cloud services (68% agreement),

(7) encourage Member States to achieve a greater consistency and clarity in their public procurement processes (68% agreement),

(8) enable a level playing field for data sovereignty both inside and outside Europe (67% agree),

(9) improve legal frameworks, for example the exchange of health information between hospitals or doctors could be done more cost efficiently and securely through the cloud (48% agree).

Respondents stress the need for a pragmatic approach that effectively protects data in the cloud. A review of existing legislation and policies in various countries and sectors is necessary to achieve this goal and to eliminate needless barriers in the Digital Single Market. Data protection legislation is a key consideration, just as other laws or policies that emphasise formal requirements (e.g. data location) rather than the underlying functional requirements (e.g. security or accessibility). A technology oriented approach is also needed: strong encryption, identification and authentication may be the most effective tools to protect cloud data and to ensure trust.

Effective dispute resolution remains challenging in the cloud business. Accessible model terms of reference could be beneficial, but in addition new efforts are needed to promote alternative dispute resolution mechanisms oriented towards consumer protection.

The respondents recognize the need for a stepwise approach that takes into account the different sensitivities and complexities of the potential use cases. There is no one-size-fits all solution to cloud computing challenges, and a big bang adoption of cloud solutions across any given sector is usually impossible. The initial emphasis should be on identifying existing solutions and best practices, promoting these, and then to gradually work on eliminating any remaining legal, political, and technological barriers. Best practices should respect and promote the existing multiplicity of technologies, business models, and provider types.

Any future initiatives in relation to cloud computing need to carefully consider the inherently international and highly innovative nature of the cloud. This implies that policy measures should avoid creating needless borders or limitations for cloud providers, including by creating mandatory compliance obligations that would harm SMEs.

Transparency is key. The cloud sector does not need to be pushed towards new technologies, business models or standards. It will continue to develop and apply these on its own. However, the market could benefit from measures that make existing

solutions easier to understand and assess by (potential) consumers, so that it becomes easier for them to select the right cloud providers.

5. CONCLUSION

In order to determine in a more comprehensive manner whether these ideas are widely supported, and to identify the most effective means of achieving them, the Commission services are minded to organise a formal consultation of policy options in the area of cloud computing to stimulate a deeper debate at European level. This would be a practical way to implement the European Cloud Partnership Steering Board's recommendation that a wider engagement through consensus building processes is needed.

Relevant parties (including: Member States, European Parliament, European Economic and Social Committee, Committee of the Regions, Cloud Service Providers, Technology and Legal Industry Bodies, User Associations and NGOs/Civil Society) would be invited to participate in any consultation process and debate on desirable future actions.

Annex

1. TRUSTED CLOUD EUROPE REPORT FROM THE EUROPEAN CLOUD PARTNERSHIP STEERING BOARD

http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4935

2. QUESTIONNAIRE

2.1. Table of Questionnaire Responses

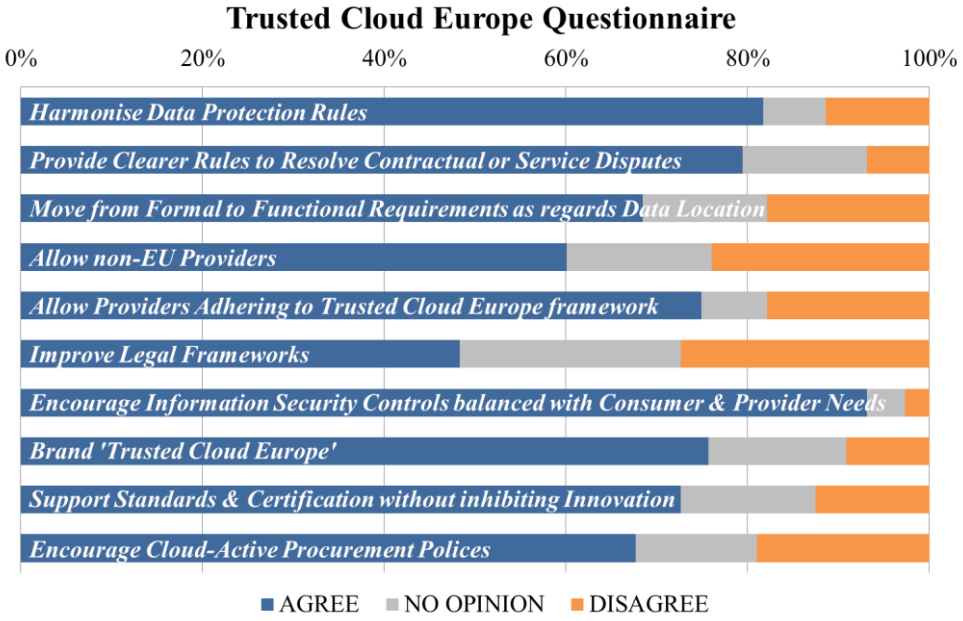
The majority (252) of questionnaires were completed through the online tool and 11 were also included directly with email responses. This table shows the total responses of all 263 received. The questions were taken from Trusted Cloud Europe and the relevant page number is also listed in below.

Question	AGREE	NO OPINION	DISAGREE
1. "The lack of full EU harmonisation of data protection rules is a recurring legal barrier." (page 10)	215	18	30
2. "Given that particularly citizens and SMEs have limited resources for engaging in legal proceedings, enforceability depends on the establishment of a credible and accessible dispute resolution mechanism." (page 18)	209	36	18
3. "Even outside of formal laws, norms may exist (issued by supervisors, regulators, sector organisations etc.) which stop or discourage the use of cloud services outside national borders." (page 11)	180	36	47
4. "It is clear that the economic potential of European cloud services depends on the ability to avoid any semblance of a 'Fortress Europe' model where access to the European cloud market is de facto restricted to providers established in the EU." (page 16)	158	42	63

5. "Non-European cloud providers should be able to access the European cloud market on equal terms, and offer services that adhere to the best practices proposed as a part of the Trusted Cloud Europe framework, i.e. functional requirements in relation to data type, data usage and enforceability of European laws and fundamental principles." (page 16)	197	19	47
6. "Privileged information can be protected by legal frameworks that stop cloud adoption or limit use cases." (page 10)	127	64	72
7. Providers and consumers of cloud services need "technological security and access control solutions, including - where proportionate - strong encryption technologies, systematic logging, time stamping, and automated breach detection measures". (page 15)	245	11	7
8. If Trusted Cloud Europe were to "become a recognizable brand and a mark of quality for cloud vendors", this would create "an additional selling proposition on the global market for cloud services." (page 17)	199	40	24
9 "Ad-hoc checks [for legal norms, data control, security certification and accountability] are not always financially or operationally viable, especially for citizens or SMEs that lack the know-how and economic resources to conduct such checks." (page 16)	191	39	33
10. As cloud computing could create significant cost savings, Chief Information Officers of every Member State's administration should aim "to change the mind-set of procurers, to stimulate cloud adoption, and to ensure that the benefits of the cloud can be maximized by re-using successful services whenever possible" through adopting cloud-active procurement policies. (pages 18-19)	178	35	50

2.2. Questionnaire Responses Chart

The responses to the questions are shown in the table below with category headings to summarise those questions.



3. COMMUNITY TOPICS

https://ec.europa.eu/digital-agenda/en/content/trusted-cloud-europe-survey-discussion-group

3.1. Small and Medium-sized Enterprises (as users and suppliers)

The report states the following (page 16):

"Facilitating the cross-border recognition of these best practices. Adherence to these best practices should be verifiable and auditable without extensive case-by-case checks, since ad-hoc checks are not always financially or operationally viable, especially for citizens or SMEs that lack the know-how and economic resources to conduct such checks. Therefore, the use of self-declaration, third party audits and one-stop-shop certification/trust marking schemes should be supported where appropriate as a tool to make adherence against the aforementioned best practices, accessible to as broad a market as possible. Any endorsed certification/trust marking practices should be industry driven and customer centric, voluntary, lean and affordable, technology neutral and based on global standards wherever possible, in order to avoid needlessly increasing costs, especially for SMEs."

What do you think?

3.2. Data Location Restrictions

The report states the following (page 19):

"Reduction of data location restrictions: Member State practices and in some instances national laws restrict the possibility of storage and processing of certain

data (especially public sector data) outside their territory. If common requirements can be found for similar use cases, Member States can choose to gradually phase out data location restrictions when they are deemed unnecessary. This does not imply that data controls should be abandoned; it is often possible and advisable to replace formal legal requirements (such as geographic location of the data) by the corresponding functional requirements (such as ensuring the accessibility and security of the data). State-of-the art security technologies could be regarded for some use cases as an alternative to data location restrictions. This goal oriented approach is technologically neutral, conducive to supporting innovation and new technologies, and enables public policy objectives to be more effectively reached."

What do you think?

3.3. Procurement Practices

The report states the following (page 19):

"Alignment of procurement rules and practices: Procurement rules in some Member States can make it difficult to sell cloud solutions to the public sector. This is burdensome to public administrations, which can be barred from technologically and economically advantageous solutions, but also for cloud providers, who are faced with different requirements from country to country. By sharing best practices, Member States can ensure that their procurement legislation and policies will become cloud enabled. Furthermore, they could work towards developing common approaches to public procurement of cloud computing, or towards the mutual recognition of any existing national accreditation schemes, so that providers do not need to seek different certifications, accreditations or approvals in different Member States. Similarly, Member States can share effective national budgeting policies to ensure that pay-as-you go models (moving from capex to opex) can be enabled."

What do you think? Is this the right approach for IT/cloud procurement? Are these the right actions for procurement? Are there missing actions? What is the most important action on this topic? Who are the most important stakeholders as regards procurement?

3.4. Cloud-Active Procurement Policy

The report states the following (page 18):

"…consultations and workshops should help citizens, businesses and Member States to build a consensus on their challenges, as dictated by their individual interests and backgrounds, and to seek common solutions, building on best practices in the cloud market. An example of the latter are cloud-active procurement policies which have been adopted by some Member States. While details vary from country to country, such policies generally require administrations to at least consider cloud technologies (including both public and private clouds) for their IT procurements, and to ensure that their requirements do not needlessly exclude cloud technologies. The objective of such policies is to change the mind-set of procurers, to stimulate cloud adoption, and to ensure that the benefits of the cloud can be maximized by re-using successful services whenever possible."

What do you think?

3.5. Adherence to Best Practices

The report states the following (page 17):

"The Steering Board furthermore encourages the EU, Member States and cloud industry to seek out opportunities to support adherence to best practices (including both self-declarations of compliance and third party certification), and to promote the use and value of appropriate certification schemes. A flexible and innovation friendly approach will be crucial during these efforts, as the risk of elevating existing practices to the status of obligations – thus creating future legacy problems and disrupting the potential for new innovations – must be avoided."

What do you think?

3.6. Building Consensus

The report states the following (page 17):

"Consultations and workshops need to target non-legislative regulators, supervisory bodies, professional bodies and trade associations… cloud users, including citizens, SMEs and larger businesses… Member States."

What do you think?

4. COMMUNITY DISCUSSION AND EMAIL REPONSES

More detailed analysis of the responses received through community discussion and via email confirmed the initial analysis and highlighted on which of those priorities the European Commission should focus. The summary below provides an overview of the principal feedback by respondents.

4.1. Encourage Information Security That Is Balanced With Consumer And Provider Needs

Any actions in relation to security controls should be strongly aligned with the EU's broader actions in the area of information security.

Specifically, one respondent noted that the proposal included in the Cyber Security Strategy of the EU, calling for the development of security labelling systems, should be built on in future cloud actions as well, as a way to simplify the understanding of security and to support diversity in security levels for different cloud use cases.

The legal framework of Regulation (EU) No 1025/2012 of 25 October 2012 on European standardisation was also referenced as a useful umbrella for potential future action, due to its integration of SME participation and compliance with WTO principles.

Finally, strong identification and authentication is crucial to the reliability and security of any cloud service. A response from Estonia stressed that a wider use of strong electronic identity and various secure technological solutions offers

opportunities for the development of higher value-added and secure services. European cloud service providers could be encouraged to make better use of existing technologies.

4.2. Support Application Of The Data Protection And Data Privacy Framework With Particular Relevance For Cloud Computing And Harmonisation Of The Framework Across Europe

The incomplete harmonisation of European data protection rules was a well-known and recurring topic in the TCE report, and was also repeatedly referenced in the feedback received in the survey. Separate cloud rules or policies on this point were not seen as necessary or beneficial. Rather, there was a strong call for completing the ongoing harmonisation work as quickly as feasible. The key priorities should be to retain strong privacy rules in order to support consumer trust, but also to ensure that the new rules are conducive to a rapidly evolving cloud-based international business environment.

4.3. Support Standards And Certification Without Inhibiting Innovation

As was also stressed by the TCE report's analysis of use cases, cloud computing is not a monolithic industry and best practices cannot be of the "one size fits all" variety. Best practices, when formulated, should respect and promote the existing multiplicity of technologies, business models, and provider types. The goal should not be to eliminate this variety, but to ensure that appropriate solutions are chosen for each use case.

To this end, mechanisms should be created that allow cloud users to assess that the right practices are being implemented and respected by cloud providers (i.e. metrics and thresholds, standards, protocols, etc.). Third party certification services can play a strong supporting role in achieving this goal, making it easier for cloud providers to show their compliance with best practices, and for cloud users to determine whether they have chosen the right service provider.

Finally, the flexibility, agility and rapid development of cloud services needs to be considered in any future policy actions. Business models, technology, standards and contract terms and conditions are still developing and changing quickly. It could be harmful to define strict models and final best practices at too early a stage. It should certainly be avoided to make the adoption of such practices mandatory, as this could significantly harm innovative players, including especially Europe's cloud SMEs. Several respondents stressed their support for internationally recognized, voluntary and transparent self-compliance mechanisms with third party verification where necessary and beneficial, to demonstrate compliance with security and privacy standards. Cloud providers operating across national borders – the default case in this industry – should not be forced to needlessly duplicate efforts in this respect, e.g. by being subjected to functionally identical auditing or certification requirements in different jurisdictions.

4.4. Review Data Categorisation And Impact Of Existing Legislation, In Order To Identify Formal, Legal And Technological Requirements, Including Data Location Requirements, And Identify Possible Functional Requirements That Could Serve As Acceptable Substitutes In Order To Further Develop Trusted Data Flow Within The Digital Single Market For Cloud Services

While a "European Cloud", whatever its exact definition, would not conclusively prevent unlawful access to data it could ensure that data and business secrets are governed and protected by the fundamental principles of law of the European Union. The European Commission should also strive to harmonise relevant EU level legislation in relation to the Digital Single Market wherever necessary to achieve this goal.

An insufficiently nuanced common framework could unfortunately serve as a limitation, as opposed to facilitation, of cloud adoption in the EU. In order to mitigate this risk, appropriate policy action should not be based purely on legislation. It should also try to leverage the knowledge and experience of non-legislative authorities and bodies. Some respondents suggested that a more effective approach would be to focus on technology oriented solutions.

Technical developments (advanced cryptography and security mechanisms) could help not only to provide strong access control, but also to enhance the privacy of data stored, and actions performed, by citizens and industry in the cloud.

NESSI stressed this perspective in their feedback, noting that "trust is a key factor for cloud adoption, regardless of countries or sectors, as information may no longer be hosted and processed on the data owner’s premises."

Ensuring security through functional requirements (including technological controls) rather than through legislation or policy-making may therefore be advisable, and lead to the gradual elimination of national borders inhibiting trusted data flow. This evolution was noted by several respondents to be a precondition for the Digital Single Market, international trade and the competitiveness of European companies operating internationally.

Finally, the importance of a stepwise approach was emphasised by some respondents, taking into account the different sensitivities and complexities of the potential use cases. In the Norwegian public sector, the Agency for Digitisation recommends that potential cloud users in the public or private sector start small, with use cases where the risk is low. To support this process, the Agency has published a set of public sector cloud computing best practice cases in the Nordic region (www.norden.org/cloudcomputing).

4.5. Provide Clearer Rules To Resolve Contractual Or Service Level Agreement Disputes

Effective dispute resolution remains challenging in the (almost) inherently international cloud business, especially given the large imbalance of negotiating power between provider and consumer. One respondent noted that the creation of (non-mandatory) accessible European terms of reference documents could be beneficial, in combination with an appropriate labelling scheme (comparable to the EU Ecolabel).

Other respondents similarly stressed the scope and importance of existing initiatives. With Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer alternative dispute resolution (ADR)), a dispute resolution mechanism oriented towards consumer protection is currently being developed. The experience of the ADR Directive should be taken into account in any future actions. Similarly, awareness of existing general dispute resolution mechanisms should be increased, both with cloud users and cloud providers. The use of existing mechanisms, with appropriate enhancements if needed, was noted to be preferable to the establishment of a sector-specific dispute resolution mechanism for cloud.

4.6. Encourage Member States To Achieve A Greater Consistency And Clarity In Their Public Procurement Processes

Finally, respondents generally encouraged the Commission to continue educating consumers and businesses about the potential benefits of the cloud. Cloud-active procurement policies could help proceed towards this goal, although correspondents cautioned against any protectionist policies that would exclude appropriate cloud providers from the European market on the basis of unjustified criteria.