Final minutes from the European Cloud Partnership Steering Board meeting

Berlin, 14 November 2013

Main conclusions from the meeting:

- The Steering Board is generally supportive of the Shared Data Area's principles as a tool for achieving an **Internal Market for cloud services**. The name as such would however need to be changed, as 'Shared Data Area' raises unfounded expectations and concerns.
- The Steering Board sees a need to **significantly speed up ongoing cloud actions** to capture the momentum created by the favourable Council conclusions. It is noted that a more or less **stable and mature ECP report would be needed by the middle of February**, with a view of presenting this to the Council to safeguard this momentum.
- The Steering Board members declare their **willingness to convene in late January/early February** to ensure that such a report to be completed; the date has been set to **13 February 2014** after the meeting. The Board members declare that they will provide the necessary support to assist in the preparation of this report.
- It is agreed that further work is needed in particular around **three items, for which work streams are to be set up** within the ECP:
  - **Private sector working group European Cloud Area:** identification of key barriers and potential solutions for cloud providers and SME users, classified in terms of different use cases and data types. A priority list of actions should be identified where fast and high impact progress could be made.
  - **Public sector "due diligence" working group:** examining rules that prevent data moving into the cloud and from flowing across borders. It should not only identify barriers but also possible ways to move forward. Again the analysis should include a hit list where fast and high impact progress could be made.
  - **Working group on identifying public sector projects where pilots can be made operational in the short term**, based where possible on cloudifying existing or planned projects.
- The Steering Board members affirm that their **Sherpas will commit to participate to these work streams** with a view of producing the aforementioned report in a timely fashion.

The Steering Board meeting was organized in conjunction with the launch event of the Cloud4Europe project, kicking off in Berlin on 14-15 November 2013. The Steering Board convened on 14 November from 8h00 to 10h30, with the following agenda:

Agenda	
8h00-8h10	Welcome address by President Toomas Hendrik Ilves
8h10-8h20	Welcome by Neelie Kroes, Vice-President of the European Commission, responsible for the Digital Agenda for Europe, including a summary overview of the Council conclusions with respect to cloud computing
8h20-8h35	Presentation of the discussion paper on the Shared Data Area by the rapporteur H. Graux, and the main open questions and issues to be decided by the Steering Board
8h35-10h00	Discussion on the Shared Data Area and next steps by the Steering board
10h00-10h10	Update on the status of ongoing Select Industry Group activities and outputs – Service Level Agreements (SLAs), Certification Schemes and Codes of Conduct, by Ken Ducatel (Head of Unit)
10h10-10h20	Wrap-up and main conclusions by the rapporteur, including a summary of agreed next steps
10h20-10h30	Concluding remarks and closing of the Steering Board meeting by Pres. Ilves

Minutes

Introduction

The Steering Board members are welcomed by M. Michael Hange, who briefly presents the agenda. The general scene of the meeting is set, including the political climate around cloud computing, ICT security and eGovernment clouds in particular. President Toomas Ilves stresses the negative impact that recent uninformed media coverage has had on trust in clouds. There is a need for a more informed debate to counter the tendency to favour purely national clouds.

Both President Ilves and Vice-President Neelie Kroes welcome the recent Council conclusions, and note their outspoken support for cloud initiatives and in particular the European Cloud Partnership as key instruments for achieving a single internal market for cloud services. The present meeting should identify our next actions, mixing low hanging fruit with longer term objectives, keeping in mind the need to enable both expedient action and the next Commission's agenda.

Report and discussions on the Shared Data Area

The rapporteur Hans Graux presents progress and open questions around the Shared Data Area. It is clarified that the SDA is seen as a possible tool to enable the Internal Market for cloud computing. Established principles of the SDA are presented, along with the main potential strengths and weaknesses, on the basis of the discussion paper, which is included in attachment to these minutes.

A discussion of this presentation follows, led by President Ilves, who stresses the importance of data integrity as a key underemphasized principle for clouds (in addition to security and privacy, which are more generally recognized by the public). Technical solutions, including advanced encryption technologies which are available today, can help achieve this goal.

M. Reinhard Posch provides a presentation to illustrate some potential cloud use cases in the public sector, and suggests that the SDA should perhaps be approached as a technological perimeter (including identity management and security measures) that all Member States could take up for their own clouds; these common technical conditions would possibly be a more useful starting point for further actions than a shared data area concept. Use cases of particular interest to the public sector would be:

- Cloud enabled electronic identification and encryption;
- Government oriented communication suites, notably secured mail and calendar services;
- Data storage and archiving;
- Cloud document management services for Europe.

While these examples are positively received, there is concern around creating a cloud oligopoly. Many of these services are commercially offered by the market; the main challenges revolve around cross border selling and removing barriers to the Internal Market. Any measures supported by the ECP should be accessible and implementable for SMEs as well and be based on existing international standards and practices, wherever possible.

The discussions emphasize the need to clarify the use cases that we need to work on. These should cover both public and private sector needs, as an assumption that the public sector will be the first adopter as we envisage them may prove to be incorrect. There is a clear need to better understand the barriers (including legal, operational, political and technical) in moving to the cloud and in offering cloud services; this would require separate work streams for the public and private sector as their challenges may differ. However, the ultimate outcome should be a single and harmonised set of actions, working on the needs of both the public and private sector and aiming to establish a fully functioning Internal Market for cloud services.

The nature of the required actions is discussed by the members, and there is a strong consensus that the initial priority should be to work on a soft (i.e. non-regulatory) approach that identifies low hanging fruit and quick wins. These include the completion of existing work (mapping standards, establishing a code of conduct with endorsement by the Article 29 Working Party, standardised SLAs and cloud certification schemes), but also the identification of use cases and the identification of barriers that need to be worked on.

Regulatory action around clouds at the EU is premature and unrealistic in view of the ECP's agenda and need for quick progress. A nimble soft opt-in approach is required, without ties to any legal changes or to the reform of the data protection legislation, which has an unpredictable calendar. A useful first step would be to encourage a due diligence exercise in all participating Member States, in which they identify which barriers to the cloud remain in their own countries; such an exercise has recently been initiated in Norway.

The Steering Board members note their general support for the discussion document, and consider it an appropriate starting point for further action. It is however noted that the term 'Shared Data Area' is misleading and has unfavourable connotations, suggesting that data will be shared with third parties, and that a physical area would be targeted. An alternative will need to be sought (such as e.g. European Cloud Space). Implementing actions will need to follow quickly, since we need to be able to capitalize on the momentum created by the Council conclusions.

The general goal of establishing a fully functioning Internal Market for cloud computing needs to be stressed. In practice, the cloud market remains fragmented at this time: the location of data is often seen as critical, especially in the public sector, not only because of security reasons, but due to restrictive regulations in this regard, and due to the problems administrations face when procuring a cloud service. We must avoid any 'Fortress Europe' perception that isolates European clouds from international markets (or bars access to them to international service providers). Security, integrity, accessibility and control over clouds must be ensured, but the members agree that geographical location is not a necessary component of these high level requirements; strong encryption based on open and established algorithms could achieve better results than geographic restrictions. There is a need in the cloud market to move from trusting companies to trusting standards and systems.

This also requires us to understand the use cases and barriers better; both the threats and opportunities need to be identified, and the past ECP actions have not yet achieved these goals to a sufficient degree. If the SDA can be reoriented towards these priorities, most Steering Board members – with some exceptions, including France, which favour other priorities such as the definition by Member States of common requirements and the support of the development of the European cloud industry through R&D programs – are supportive of continuing the work around the SDA under a more suitable name.

Future actions

It is agreed that further work is needed in particular around three items, for which work streams are to be set up within the ECP:

- Private sector working group European Cloud Area: identification of key barriers and potential solutions for cloud providers and SME users, classified in terms of different use cases and data types. A priority list of actions should be identified where fast and high impact progress could be made.
- Public sector "due diligence" working group: examining rules that prevent data moving into the cloud and from flowing across borders. It should not only identify barriers but also possible ways to move forward. Again the analysis should include a hit list where fast and high impact progress could be made.
- Working group on identifying public sector projects where pilots can be made operational in the short term, based where possible on cloudifying existing or planned projects.

The Steering Board members agree that the ongoing and planned cloud actions need to be speeded up significantly to capture the momentum created by the favourable Council conclusions. A more or less stable and mature ECP report would be needed by the middle of February, with a view of presenting this to the Council to safeguard this momentum. The Steering Board members declare their willingness to convene in late January/early February to ensure that such a report to be completed, comprising the items outlined above, and declare that they will provide the necessary support to assist in the preparation of this report. The Steering Board members affirm that their Sherpas will commit to participate to these work streams with a view of producing the aforementioned report in a timely fashion.

Wrap up

The state of the art for key actions (SLAs, certification schemes and Codes of Conduct) is briefly presented by Ken Ducatel; the need to accelerate this work (insofar as feasible given its dependences on outside actors) is reiterated. The rapporteur provides a wrap-up of the general findings; the Steering Board members agree that minutes and presentations of the ECP may be shared externally, including via constructive tweets or blog posts.

President Ilves closes the Steering Board meeting at 10h40.

ANNEX - Discussion document on the Shared Data Area

For discussion by the

Steering Board of the European Cloud Partnership

A. What is the Shared Data Area?

While an EU-wide single market for cloud computing should be the clear objective, not all Member States may be prepared to take the necessary steps to make this happen. The pathway towards a fully functioning single market for cloud computing could be a voluntary Shared Data Area, akin to the Schengen Area, where a group of Member States that are eager to realize the scale economies in the cloud could set common requirements to overcome existing data location restrictions.

1. Context: Europe must establish a fully functioning internal market for cloud computing

The potential economies of scale in the cloud can only be realized within a truly-functioning EU-wide single market for cloud computing. Decisive measures would be required to overcome the current fragmentation in European cloud markets.

Harmonization of EU Data Protection Rules: The implementation and interpretation of the EU Data Protection Directive differs significantly from Member State to Member State. A cloud provider required to comply with multiple national data protection regimes when offering EU-wide cloud services. This is a huge challenge for large vendors and most of the smaller providers simply cannot afford or manage this. Equally, public administrations and business users have compliance concerns when storing their data outside their home country given the complex legal environment and related liability issues. It should therefore be made easier for cloud users to choose providers known to be compliant, e.g. on the basis of certification or trustmarking, as this is an obstacle for the take-up of cloud computing. The further harmonization of data protection rules in Europe must be completed urgently, as foreseen within the ongoing negotiations on a EU Data Protection Regulation, as a powerful enabler for a single market for cloud computing.

Data locations restrictions: While the current EU Data Protection Directive allows for the transfer of personal data under certain established conditions, there are additional practices in Member States and in some instances national laws[1] that restrict the possibility of storage and processing of certain data outside their territory. It is common practice among public administrations to store and process data within their respective national territory. Public sector cloud initiatives, such as the so-called G-Cloud, have not yet changed this practice. Similar data location restrictions exist for health records, taxation related data, financial services, social security, labor contracts and public administration archives.

[1] For example, hospital data in Belgium is required to be kept within the respective hospital or in a Belgian database held by the Ministry of Public Health. Art 20 of the Act on Hospitals of 10 July 2008; Royal Decree of 27 April 2007 on Hospital Records.

The new EU Data Protection Regulation is expected to help overcome some of the data location restrictions regarding personal data in the EU. Nevertheless, the motivations for these restrictions go beyond data protection. They relate to jurisdictional uncertainties and to the difficulties for business and public sector cloud users to enforce their regulatory obligations in another member state. Member States and relevant stakeholders should therefore verify the actual need of these restrictions and elaborate on ways to resolve them in order to improve the free flow of data and enable economies of scale in the cloud. Cloud computing can provide users with powerful security tools, including easy to use, end-to-end, advanced encryption technologies. Especially SMEs can benefit from getting the latest security technologies as a service in the cloud that they often cannot afford when operating their own IT systems. Therefore, state-of-the art security technologies could be regarded at least for some use cases as an alternative to data location restrictions.

Public Procurement: The implementation of European public procurement rules for cloud computing services differs from Member State to Member State. This situation is burdensome especially for smaller cloud providers and hinders them from participating in public tenders across the EU. Member States should be encouraged to adopt common approaches to public procurement rules for cloud computing, and where appropriate take Cloud Certification Schemes into account. The identification of good practices with respect to cloud technical requirements (including their link to certification schemes) could thus increase competition and vendor choice for public administrations.

2. Member States should consider the creation of a Shared Data Area in the Cloud

Finding the appropriate balance between data location restrictions and scale is the primary reason of a Shared Data Area. Obviously, the governance structure, the business case and the technical implementation of such a Shared Data Area need further analysis by those Member States that are willing to pursue this opportunity. The following principles for a Shared Data Area could apply:

- The Shared Data Area would be established on an opt-in basis by Member States. It would be open to additional Member States to join at a later stage.
- The Shared Data Area would be based on an agreed set of principles for the transfer, storage and processing of data to enable the free flow of data within the designated area.
- The Shared Data Area would allow for the development, provision and use of local, regional, national and cross-border public services by participating Member States.
- The Shared Data Area must be fully compliant with EU laws and especially with EU Data Protection rules.
- The Shared Data Area should not preclude the transfer of data to third countries, provided that adequate level of data security and data protection in full compliance with EU law is ensured, and provided that the transfer is approved by the cloud user.

Participating Member States would consider:

- Reviewing applicable laws and practices that restrict the transfer, storage and processing of data outside the respective Member States to enable the use of the Shared Data Area and facilitate the establishment of a set of agreed principles and protocols.
- Establishing of framework of mutual assistance so that regulatory authorities can enforce applicable legal obligations when the respective data is located outside the respective country within the Shared Data Area, and ensuring that this framework is consistent with EU data protection law and especially with the envisaged cooperation between national data protection authorities under the new EU Data Protection Regulation
- Designating part of any closed government clouds for the Shared Data Area.
- Establishing a “one-stop-shop” European compliance certification mechanism for cloud services through co-ordination among participating Member States to ensure an adequate level of data security, data protection, disaster recovery and overall service quality. This regime should also help to address liability concerns of cloud users and vendors/providers alike.
- Initiating pilot projects in targeted areas (ex: public sector information, healthcare, etc.) based on common requirements. Less sensitive areas (e.g. research and certain education related projects) could make for interesting pilots and generate acceptance.

Furthermore, public procurement for the Shared Data Area should be open to providers from inside and outside the EU, provided they meet the requirements of the SDA as defined by participating Member States.

B. What are the potential benefits and downsides of the Shared Data Area?

1. Potential benefits of a Shared Data Area

The following benefits could be expected from the Shared Data Area (in some cases depending on implementation choices as laid out below) :

- Compliance with applicable laws (including data protection) is facilitated for cloud vendors and cloud buyers, through a common understanding of rules and through increased harmonization of technical requirements; internal market access is facilitated since a EU-wide cloud vendors no longer need to comply with multiple cumulative legal frameworks.
- Trust is increased through common Codes of Conduct, commonly identified standards, and possibly common certification practices, which should be voluntary, lean and affordable, technology neutral and based on global standards (ISO 27001, 9001, etc.) wherever possible.
- Procurement of cloud solutions is facilitated for public sector buyers by establishing common purchasing criteria which are logically linked to their use cases, data types and the resulting security needs.

- SDA-compliance could become a mark of quality for European cloud vendors and thus create an additional selling proposition on the global market.

- Data location requirements are removed within the SDA. While fully respecting international free trade rules and in a spirit of openness, the SDA removes any need for MS to keep their data/services within their internal cloud, thereby missing out on the scale effects of the cloud.

- The SDA can be adopted by public and private sector users alike, allowing good practices to spread easily.

2. Potential downsides of a Shared Data Area

The following downsides could be expected from the Shared Data Area (in some cases depending on implementation choices as laid out below) :

- The SDA can create a 'Fortress Europe' situation where access to the European cloud market *de facto* is restricted to EU providers; could inhibit international free trade.

- The SDA's link to data protection and national security is a risk, as discussions are volatile and sensitive; e.g. access to cloud data by governments is not controllable by cloud vendors.

- Costs of compliance may increase, especially if certification or inappropriate standardisation is an integral part of the SDA; this would be bad for SMEs and European competitiveness.

- Expectation management is required: would removing data location restrictions solve MS' tendency to keep data/services within their internal clouds? These tendencies to keep data in internal clouds may be caused by other factors than (domestic) (legal) compliance concerns, e.g. disadvantageous foreign law in the field of bankruptcy or investigative powers.

- SDA implies that MSs voluntarily join; this may be complex and risks creating a schism between 'SDA MSs' and 'non-SDA MSs', harming the internal market.

C. What aspects of the Shared Data Area need clarifications or decisions from the Steering Board?

1. Is the SDA a goal in its own right, or an outcome of internal market actions?

Do we present the SDA as the main initiative to be taken by all stakeholders (Commission, Member States and Industry) which comprises a set of measures as outlined above, or do we focus on proposing a set of internal market measures that will result in an SDA?

2. Is the SDA fundamentally about eliminating data location restrictions?

Does this goal require the complete elimination of such rules (including through national legislative reform)? And is the implication that the SDA forms a single 'virtual' area in which the data may move (but which the data may not leave)? Moreover should the SDA be about *implementing security controls that ensure equivalent protections to local storage rather than physical location per se?.*

3. How strong is the link between the SDA and Data Protection reform?

First, can the SDA be seriously considered before the data protection reforms are complete? Or is it the case that primary goal of an SDA is to facilitate compliance for cloud vendors and cloud buyers (including Member States), i.e. choosing an SDA-compliant vendor would shield the buyer from liability. Is that indeed our goal?

4. Should the SDA target the public and private sector equally?

What is the right balance in the approach to the SDA between a public sector or industry focus. Should we focus the SDA as a public sector targeted measure (facilitating cloud adoption for Member States), while allowing the private sector to adopt it voluntarily?

5. Can the SDA be defined to apply across various business/administration contexts, or do we need to take a context by context approach?

Different types of data have different needs: would an SDA immediately apply to general contact data, business information, fiscal data, health data, transportation/mobility data, etc? What is the link to meta-categorisations such as personal data, open data, public sector information, etc? Do we need to take a step-by-step approach, including common definitions?

6. Is the SDA a 'hard law' approach, or a 'soft law' approach?

Will Member States be required to systematically review and (if necessary) change their laws as a condition to signing up to the SDA, or is the SDA focused on creating and promoting voluntary best practices? Furthermore, how can jurisdiction issues be addressed without 'hard law': data hosted in a foreign country may become accessible to competent authorities in other Member States. Is that acceptable, and if not, how can this be managed?

7. Who will champion the Shared Data Area within the Steering Board, including both Member States and Industry?

Adoption and support needs to be clear, as well as a consensus on how the SDA will be implemented by the champions.