

Minutes of the plenary meeting of the Cloud-Select Industry Group (C-SIG)

29 October 2015, 10h00 – 17h00, BU25, Brussels, Belgium

SUMMARY

The European Commission presented an overview of the initiatives that are most relevant for cloud computing under the Digital Single Market (DSM) Strategy (the Free Flow of Data initiative, the European Cloud initiative and the Interoperability and Standards initiative) as well as on-going action on standards, security certification, contract terms and conditions, and the draft Data Protection Code of Conduct for cloud service providers. A summary of key market trends and projected growth paths for cloud computing in Europe was set forth by Deloitte.

C-SIG members were invited to comment on the draft reports issued by ETSI on standardisation and on the preliminary results presented by Deloitte on the economic impact of cloud computing in Europe. C-SIG members are also invited to contribute to the on-going public consultations on data, cloud computing and standards, which are open until 30 December 2015.

C-SIG members agreed to move ahead with the finalisation of the Code of Conduct to align with the Article 29 Working Party's (WP29) Opinion. The Code of Conduct will be a living document that could help to avoid diverging interpretations of EU Law in the field of cloud computing. Even without formal endorsement of WP29, an industry code will have a market value, as it can help to demonstrate accountability (which is a key principle in the GDPR), give confidence to cloud users and support them in their risk assessment. The Code would benefit from an endorsement and support from cloud users and other user representative organisations and from the support of the C-SIG. C-SIG members who are willing to contribute to the finalisation of the Code of Conduct were invited to join the drafting team that will work to align the Code with the recommendations of the WP29 and to improve the governance structure.

C-SIG's future work should be mapped against the DSM Strategy. The European Commission will set up a coordination meeting between C-SIG members after the closing of the public consultations on data, cloud computing and standards in order to define the C-SIG working groups to maintain or create and to clarify their responsibilities and synergies.

1. WELCOME AND INTRODUCTION

Pearse O'Donohue (Head of Unit "Software and Services, Cloud" - **POD**) opened the meeting and welcomed the participants. He recalled that the Commission had put an ambitious agenda on the table in the Digital Single Market Strategy published in May 2015. He pointed out the links between cloud, the DSM Strategy and the C-SIG's role. He thanked participants for their continuous collective effort and introduced the agenda for the day. He invited the participants to provide input and to raise any issues faced by the industry along the plenary meeting.

2. STANDARDISATION

Dan Chirila (DG CONNECT - **DC**) presented the activities of the European Telecommunications Standards Institute's (ETSI) Cloud Standard Coordination (CSC). He stated that at the end of CSC Phase 1 ETSI concluded that there was no jungle of standards but identified some gaps and issues. He explained that a CSC Phase 2 has been launched to address those gaps and issues, focusing on four priority areas: (1) user needs, (2) security, (3) standards maturity, and (4) open source & open standards. DC provided a snapshot of the objectives, deliverables, timeframe and status for each of these priority areas. Draft reports have been available online for comments since last June. ETSI will issue its final reports in December 2015 and a final workshop will be organised the same month.

POD invited the participants to provide the Commission with their comments on the draft reports prior to the closing of the exercise with the consultants.

Joe Alhadeff (Oracle - **JA**) commented that the draft reports are not focusing on defining open standards while it was thought at some points that open standards would be the solution for interoperability issues. It was replied that ETSI reports are assisting in mapping the standards and identifying the gaps and that the Commission's focus is on how to make the decision to take up cloud easier for the users. JA also raised the importance of looking at standards as a combination of standards where, multiple standards can be used to achieve a similar goal.

Helmut Fallmann (Fabasoft - **HF**) commented that the draft reports are missing technical standardisation work on authentication. He stated that national implementations of eID are too complicated (e.g. in Germany) and lead to fragmentation. HF indicated that he sees a need for an API for smartphones that works everywhere in Europe without interoperability issues and therefore a need for binding business rules. POD referred to the eIDAS Regulation and clarified that the issue of authentication is also relevant for the European Free Flow of Data initiative and the European Cloud initiative. He indicated that the Public Services unit of DG CONNECT has plans to extend their work on CEF and eIDAS and perhaps could help to identify potential gaps. In relation to authentication POD also encouraged industry to come forward with initiatives as the Commission is bound by the principle of subsidiarity.

3. SECURITY CERTIFICATION

Mark Smitham (DG CONNECT - **MS**) gave an overview of the work done on cloud security by the subgroup of the C-SIG on certification and by ENISA. The result was the publication of a dynamic Cloud Certification Schemes List (CCSL) and Meta-Framework (CCSM), which are available on the ENISA website. The CCSM goes a step further than what was needed by the Commission to deliver its strategy to the extent that this tool also maps security requirements for cloud-based services from the national governments of 11 countries based on publicly available material. In addition, ENISA provided an online procurement tool to support SMEs and the public sector to "go cloud" and to find what certification scheme best fits their security objectives and their needs. Furthermore, MS presented the conclusions of the cloud security conference that was organised by the Latvian Presidency of the Council of the European Union in June 2015. Lastly, he referred to the Trilateral Research and Consulting study on cloud certification of 2014 and the Eurostat report of 2014 which highlight that users are still lacking trust in cloud services and possible ways to improve trust by means of certification. MS outlined that building trust in cloud services goes beyond security certification and that certification is one of the key elements of the DSM Communication of May 2015.

Thanh Nguyen (Orange - **TN**) asked whether there is any lesson learnt from the terms of reference of the tender for cloud services launched by DG DIGIT and raised that for small providers it is difficult to comply with all technical requirements. POD replied that possible negative effects for small companies of creating a single certification system would have to be prevented. MS reflected on the DG DIGIT call for tender for the acquisition of cloud services and added that under public procurement rules public authorities cannot merely require compliance with one particular standard. As an example he added that the objectives of the CCSM were to identify requirements from Member States that are similar.

As regards the security of cloud services, both Jonathan Sage (IBM - **JS**) and John Kennedy (Oracle - **JK**) concurred that cloud systems are generally more secure than the systems currently used by SMEs. Stephane Ducable (Amazon Web Services - **SD**) added that security is the reason that leads some of their customers to adopt cloud solutions. JK pointed out that certification work needs to be more user-centric. Tobias Höllwarth (Eurocloud - **TH**) echoed it and

emphasised that there is a business case behind certification. Participants agreed that certification should provide added value, being at the same time user-friendly and a selling argument, and not just an additional stamp to get.

4. CONTRACT TERMS AND CONDITIONS

4.1. Safe and balanced terms

François-Régis Babinet (DG JUSTICE - **FRB**) presented a short overview of the work of the Expert group on Cloud Computing Contracts (which was initiated by DG JUSTICE in cooperation with DG CONNECT), on the safe and balanced contract terms for SMEs and consumers. Amongst others as an outcome of the work of the Expert group, and after extensive consultations, the European Commission is now moving forward with two legislative proposals to be adopted by the College by the end of the year. These legislative proposals relate to the supply of digital content (including cloud computing) and the online sales of tangible goods respectively. They both focus on fully harmonising key rights for consumers such as conformity, quality, unilateral modification of contractual terms, and termination of long-term contracts. FRB specified that although B2B transactions were also considered in the Impact Assessment of the supply of digital content proposal, it was decided not to mix the B2B and B2C aspects together for the purpose of this current legislative proposal. The Commission may explore a different approach to tackle the B2B aspects.

Freddy Vandenwyngaert (EuroCIO - **FV**) asserted that EuroCIO is aware of significant concerns from business users about cloud contract negotiations and that standard templates would be welcome. Nicky Stewart (Skyscape - **NS**) raised on the other hand the difficulty for providers to negotiate B2B contract terms on standard services when multiple customers are all using the same service. POD concluded that while the largest members of EuroCIO might actually be able to negotiate contract terms with cloud service providers, it might not be true for SMEs, and that standard terms could support fairness and transparency.

Michael Symonds (Atos - **MS**) mentioned that the industry is aware that most public organisations and SMEs are lagging 15 years behind the private sector in terms of maturity of understanding of cloud services. As part of the learning process, it would be important to hear more from EuroCIO about what their members believe the requirements should be and to assess whether these would be realistic.

4.2. Service Level Agreements (SLAs)

Judit Schveger (DG CONNECT - **JSc**) presented the state of play of the work on SLAs. She outlined that one of the key problems for users when acquiring cloud services is to identify SLAs and also to compare similar cloud services and their service level objectives and targeted metrics. She provided an overview of the work of the C-SIG subgroup on SLAs, including the checklist and the standardisation guidelines that were agreed by the C-SIG in June 2014 and further used as additional input to the ISO/IEC 19086 project (ongoing work on an international standard for cloud Service level agreement (SLA)). JSc also referred to a study on "Standards terms and performances criteria in Service Level Agreements for cloud computing services" (SMART 2013/0039) contracted by the Commission in regards to SLAs, which could be used as an additional background document for future industry initiatives (eg. under C-SIG) and policy work by the EC as well on cloud SLAs. This study is providing a mapping of relevant legislations and best practices as well as a checklist for cloud SLAs. She also clarified that previous work under the Cloud Computing Strategy will be used as an input for future policy work under the DSM.

The floor then was opened to participants and C-SIG members were asked how they would like to move further with the SLAs under the DSM umbrella and whether the industry is currently encountering special needs or issues.

The discussion started by flagging that different initiatives exist in relation to cloud SLAs. It was however clarified that research (SLA-READY, SLALOM) and policy initiatives (collaboration between EC and C-SIG, EC studies on the same topic eg SMART 39/2013) deal with similar questions with different means or tools; such tools also address similar problems at different level. It was then raised that it is up to the C-SIG to decide whether they want to provide meaningful contribution to the ongoing work by ISO/IEC JTC 1/SC 38, eg. ISO/IEC 19086-4 is still open for industry contribution (i.e. Information technology /Cloud computing /SLA framework and Technology /Part 4: Security and privacy).

Gregory Gitsels (OVH - **GG**) pointed out that the SLAs do not take into account the specificities of an Internet Service Provider (ISP) such as OVH, and do not really fit with its activities. POD stressed out that the Commission's initiatives on SLAs are focusing on the users' perspectives to encourage their uptake of cloud services.

5. DATA PROTECTION CODE OF CONDUCT FOR CLOUD SERVICE PROVIDERS

JSc then gave an overview of the work on the draft Code of Conduct and the WP 29's recently published Opinion. She recalled the role of the Commission, which is to encourage the industry to use a self/co-regulatory approach, to facilitate the work of the industry and to increase the trust of users in the cloud services. JSc summarised the purpose and the methodology of the Code of Conduct as well as its content. She highlighted the main benefits of codes of conduct in general and more particularly its legal recognition under the current Data Protection Directive and also under the draft version of the future General Data Protection Regulation ("GDPR"). JSc stressed that the plenary meeting is a great opportunity for the C-SIG to decide on the next steps to finalise the Code of Conduct in line with the WP29's opinion.

Hans Graux (Time.Lex - **HG**), as former development leader for the code of conduct presented the Opinion of the WP29 and summarised the main issues raised. He emphasised that the WP29's Opinion is an open invitation to revise and finalise the draft Code of Conduct. None of the issues highlighted by WP29 are insurmountable, however some might be more complicated to tackle than others. In some cases, the WP29 requests explicit reference to the data protection acquis and in others, a more specific and detailed cloud perspective should be stressed as an added value to the European data protection legal framework (with specific cloud-related examples). It is critical for the WP29 that the Code of Conduct makes it clear that (i) it will in no case replace the law but it will clarify it from a cloud perspective and (ii) it will not encroach on DPAs' competencies but help them by clarifying. Given that the WP29 wishes to preserve its neutral position, it declined the invitation to be part of the governance structure of the code. In line with the Opinion, the Code should set out industry best practices to enable cloud users to verify provider's compliance with data protection rules; the Code should also provide for further clarification on self-assessment and third party certification against the Code. The challenge will be the transition towards the GDPR. The WP29 encouraged a forward-looking approach that already include provisions of the GDPR that are not part of Directive 95/46/EC and national laws (such as on liability or data portability).

POD concluded by insisting on the importance and value of the Code of Conduct to provide guidance on data protection issues in a cloud environment to both cloud providers and users. The CJEU ruling on the Safe Harbour scheme ("Schrems case") was anticipated by many stakeholders. The GDPR is now at the end game of the negotiations. He also emphasised that in line with WP29 Opinion, the Code of Conduct should be a living document. POD strongly

recommended the C-SIG to move ahead with the Code of conduct and to look at the governance structure of the code. He pointed out that the GDPR will probably be enforced 18 months after its adoption (even though Member States would not have to transpose it into their national legislations) and that it would be advisable to start already anticipating the GDPR.

JS (IBM) and JA (Oracle) endorsed POD's view. There is a window of opportunity to get the code finalised and it should be done as soon as possible as the code is an important industry-led sector specific tool. The Code also needs to be reassessed as soon as the GDPR is adopted. It appears that 50% of the WP29 recommendations can simply be included in the Code by emphasising relevant sections in the European data protection acquis, and 25% can be easily accommodated. The remaining 25% needs further clarification by the industry, to shed light on common misunderstandings about what cloud is and how cloud providers are operating (e.g. request to provide specific postal addresses where data processing is occurring). The Code would have to be able to take account of changes that will occur in early 2016: adoption of the GDPR, joint-statements by WP29 and/or national DPAs. A full understanding of the GDPR will not come as soon as it is adopted but later, once it has been enforced. The current governance model and structure of the Code of conduct should be further refined (e.g. how the code can be endorsed, managed, reviewed etc.).

Stephanie Finck (Salesforces - **SF**) indicated that the driver to set up a Code of Conduct was to have the WP29's endorsement at the first place and asked whether the code will have a value without such an endorsement once the GDPR will be adopted. Mark Lange (Microsoft - **ML**) questioned the value of a non-endorsed code for the cloud users. Daniele Catteddu (Cloud Security Alliance - **DC**) asked whether the Code of Conduct should be resubmitted to the WP29 should it be refined and whether such a resubmission would actually make sense if a governance model is in place. Other members of the C-SIG plenary (e.g. Oracle, IBM) however insisted on to finalise the Code in line with WP29's opinion in order to have a functioning code in practice as soon as possible.

POD recalled that there is a political context around the Code of Conduct and that the WP29's Opinion is addressed not only to the industry but also to the national DPAs. The industry has a close relationship with DPAs and that it will be a missed opportunity if the Code of Conduct would be put on hold. While there is no intention to resubmit the Code of Conduct to the WP29, such a possibility should not be excluded. If the C-SIG can address the majority of the WP29's concerns and recommendations, the industry can market that the Code of Conduct has been refined to line up with the WP29's opinion. Such a code could become a benchmark for the cloud industry.

POD invited the drafting team on the Code of Conduct as well as the participants who have a particular interest in the code to meet during an hour to discuss further the merits of moving ahead with the Code of Conduct and whether the majority of the WP'29 concerns could be sorted out and to then present the outcome to the plenary meeting.

It resulted from this meeting that the majority of the participants were in favour of moving ahead with the Code of conduct. It was raised that some issues would be more complex than others to solve especially when they relate to the anticipation of the GDPR (e.g. international data flows or liability). It was also suggested to extend the current drafting team.

The arguments in favour of moving ahead with the Code of Conduct were set forth in the plenary meeting as follows: (i) the WP29's Opinion is a positive feedback. The WP29 did not reject the code but identified some weaknesses to cope with. In the current context, it is unrealistic to expect a formal endorsement by the WP29; (ii) even without the WP29's endorsement, the Code of Conduct will have a market value. An industry code could help

demonstrating accountability (which is a key principle in the GDPR), give confidence to cloud users and support them in their risk assessment; (iii) the code could help avoiding different interpretation of Community Law eg. in light of the recent CJEU ruling ("Schrems case"), which reinforced the roles of national DPAs. It could indeed help DPAs to understand at the beginning of the process how the industry works; (iv) the European Commission will continue to encourage self- and co-regulatory initiatives by the industry including amongst others the role to facilitate the C-SIG work on the Code of Conduct; (v) the Code of conduct could benefit from an endorsement and support from cloud users e.g. EuroCIO and other user representative organisations and from the support of the C-SIG.

The participants agreed that the governance structure needs further work, on points such as a mechanism to allow the code to evolve over time, adherence and certification schemes (self-assessment *versus* certification by a third party), and on compliance with the code. Robust governance will increase the confidence of users and data protection authorities in the code.

It would be valuable to gather the view of the users once the draft Code of Conduct will be consolidated. Géant and the EuroCIO confirmed that they are willing to contribute. Their input should however not slow down the finalisation of the code.

Despite its merits, the possibility of annexing an explanatory memorandum to the Code should be avoided as it could become a dump for sensitive issues that could not attain a consensus.

POD closed the discussion on the draft Code of Conduct. He concluded that the C-SIG is willing to move ahead with the finalisation of the Code and that the GDPR should not be an excuse to postpone the finalisation of the Code. The next step is for the drafting team (i) to refine the Code to align with the recommendations of the WP29 that can be easily coped with, (ii) to identify the redline issues relating to the GDPR, (iii) to improve the governance structure. POD invited stakeholders who are willing to be an active member of the drafting team to contact Judit Schveger; a reminder will be sent to all participants to C-SIG plenary.

6. PRESENTATION OF THE PRELIMINARY RESULTS OF THE STUDY "MEASURING THE ECONOMIC IMPACT OF CLOUD COMPUTING IN EUROPE" CONDUCTED BY DELOITTE

Deloitte presented a summary of data on key market trends and projected growth paths for cloud computing services in Europe and worldwide, on adoption rates among businesses and on the key barriers limiting or preventing wider adoption of cloud computing services identified by business. The measures currently implemented within the European Cloud Strategy and those under consideration for future implementation by the Commission were also discussed.

Charlotte Thornby (Oracle) raised the issue of the impact of the draft NIS Directive on cloud. She added that following the CJEU ruling (Schrems case), the net benefits to the EU economy will be smaller if there is no transatlantic flow of data. She emphasised that currently there is no appropriate compliance measures to allow such data transfers.

TH (Eurocloud) shared scepticism about the deadline set by the data protection authorities. He also flagged the lack of digital skills in Europe.

7. DISCUSSION OF THE ELEMENTS OF THE DIGITAL SINGLE MARKET STRATEGY MOST RELEVANT TO CLOUD COMPUTING

Tjabbe Bos (DG CONNECT - TB) presented the DSM Strategy, and particularly the initiatives with cloud relevance, i.e. the European Free Flow of Data initiative, the European Cloud initiative and the Interoperability and Standards initiative. In relation to the European Cloud Initiative he

mentioned the Franco-German conference on the digital economy held on 27 October 2015 in Paris where President Juncker announced that the Commission will present an initiative to create a European Open Science Cloud (amongst others based on high performance computing), which may go beyond the science community and also support the use of cloud computing in the public sector. Secondly, the Free Flow of Data initiative is aimed at establishing the free movement of data across Europe, complementing the current legislation on the protection of personal data, removing unjustified legal barriers or location restrictions which prohibit data flows of various types of data within the EU (such as raw research data, data part of manufacturing process, anonymised data), and addressing emerging issues such as data ownership, access, reuse and liability. The Commission has launched a two-phased study to provide a comprehensive mapping of data location restrictions in all Member States, as well as their economic impact. He invited stakeholders to participate to the on-going public consultations on data, cloud computing and standards launched in September 2015.

POD explained that we need a European supercomputing capability to process big data coming from programmes such as GALILEO or CERN. The European Open Science Cloud will leverage existing initiatives (such as Géant). Certification will also be an essential part of it.

HF (Fabasoft) raised the issue of the lack of digital skills in Europe.

Barbara Wynne (Accenture - **BW**) asked about the scope of the European Free Flow of Data initiative, for example on its relationship with the European Cloud Partnership and whether the Commission will look at the public procurement rules in relation to cloud and whether the emerging data issues will focus on both B2B and B2C aspects. TB confirmed that the Commission's work is based on the European Cloud Partnership's report and that the Commission is examining the initiative from a broad perspective. POD added that the Commission is working to finalise the scope of the initiative and that the ambition is to increase transparency for users, make data location restrictions the exception, rather than the rule, and that the scope of the initiative goes beyond a mere public procurement standpoint.

JS (IBM) pointed out that some countries (e.g. Germany and France) are discussing a trusted cloud label to be attributed to some providers. POD replied that the countries that are imposing restrictions will have to justify them and will bear the burden of proof.

JA (Oracle) warned against using 'cloud' as a unitary term as this will not properly reflect the complexity of the different cloud modules and risk to impede innovation.

8. DISCUSSION ON THE FUTURE ROLE AND GOVERNANCE OF THE C-SIG IN LIGHT OF FUTURE WORK STREAMS AND THE IMPLEMENTATION OF THE CODE OF CONDUCT

POD asked the participants whether they are willing to continue supporting the work of the C-SIG, whether there is a need for the C-SIG to evolve or revise its role to support the implementation of the DSM, what the next actions are that the C-SIG should take, whether the governance structure is still efficient and, whether users groups should be involved.

The participants indicated broad support to continue with the C-SIG. It was found that the working process is going well and the enlargement of the C-SIG audience, with providers and users of cloud services, has been appreciated. It was found that an industry group also helps to keep track of the big picture on cloud. The geographical representation within the C-SIG appears to be fine, although it was found that there may need to be more attention for the inclusion of users of cloud services in the C-SIG work. POD welcomed this feedback and underlined that industry needs to be involved in the shaping of the DSM initiatives.

Some participants argued that there is nevertheless room for improving the coordination between the different C-SIG sub-groups, which could be facilitated by a better mapping of the projects.

Participants agree that the working group on Data Protection (including the Code of Conduct) should be maintained. Some suggestions were made as to the creation of additional working groups such as working groups on guidelines for public authorities, contractual standards (e.g. authentication, digital signature and proof of delivery in relation to SaaS), security and certification and interoperability and standards. It was highlighted that the C-SIG working groups should be mapped based on the DSM, but that a flexible approach should be taken that allows for establishment of new working streams at a later moment in time. It was suggested by POD that the C-SIG work could continue with working groups on (i) contracts and SLAs, (ii) certification, and (iii) interoperability and portability. A final decision will be made on the basis of the feedback on the DSM public consultation on data and cloud computing, which will run until the end of 2015.

As to the constituency, it was mentioned that it is difficult to involve SMEs and public services in practice in the C-SIG. The question of how to ensure that the Commission can hear the users' voice remains open. The public sector was initially represented in the European Cloud Partnership ("ECP") which was dissolved after the publication of their Trusted Cloud Europe report. Some suggestions were made such for the creation of a user's forum or the participation of national industry associations (e.g. Business Europe or Digital Europe) or public procurers to the C-SIG. POD invited the participants to send their suggestions by email.

Some participants finally mentioned that it might sometimes be difficult for them to mobilise their experts internally.

POD thanked all the participants and closed the plenary meeting at 17h00.

Speakers and Panellists:

- O'DONOHUE, Pearse – European Commission, DG CONNECT, Head of Unit and Chair
- MEDEIROS, Francisco – European Commission, DG CONNECT, Deputy Head of Unit
- STARCZEWSKI, Jacek – European Commission, DG CONNECT, coordinator of the C-SIG
- CHIRILA, Dan – European Commission, DG CONNECT
- SMITHAM, Mark – European Commission, DG CONNECT
- SCHVEGER, Judit – European Commission, DG CONNECT
- BOS, Tjabbe – European Commission, DG CONNECT
- BABINET, François-Régis – European Commission, DG JUSTICE
- GRAUX, Hans – Time.lex, former rapporteur of the Code of conduct on data protection
- WAUTERS, Patrick – Deloitte
- CILLI, Valentina – Deloitte
- VAN DER PEIJL, Sebastiaan – Deloitte
- JANOWSKI, Pawel - VVA