Minutes of the 5th meeting of the Cloud Select Industry Group (C-SIG) on Code of Conduct

12 February 2014, 13:30 – 16:30h, BU33, Brussels, Belgium

Participants:

- Ducatel, Ken – European Commission, DG CONNECT, chair
- Wodecka, Agnieszka – European Commission, DG CONNECT
- Schveger, Judit – European Commission, DG CONNECT, minutes
- Dubois, Nicolas – European Commission, DG JUSTICE

With teleconference connection:

Graux, Hans - Time.lex

1. Opening

Ken Ducatel opened the meeting and welcomed the participants. He thanked the participants for their collective effort and introduced the agenda for the day.

2. Report on the Code of Conduct for Cloud Service Providers

Hans Graux gave a brief introduction on the progress of the report. Comments from participants followed the structure of the presentation which covers all sections and subsections of the draft version of the Code:

0. Introduction

In relation to the endorsement by WP29, it was explained:

- EC was planning to publish a call for tender that would cover a number of activities to start a discussion with private sector cloud customers
- EC will involve public sector cloud customers in the context of the Cloud for Europe (C4E) project.

1. Structure
2. Purpose – ambitions of the Code and relation to applicable data protection law
3. Scope – field of application of the Code, including use cases and the CSP services

In relation to the endorsement by WP29, it was indicated that:

- ambiguous expressions such as 'mainly' or 'typically' should be avoided
- scope of the Code should have been set out the default case (data controller/processor)
- personal data was related to consumers (in a B2C relationship), this should have been clarified
- different obligations were imposed to co-controllers and joint controllers

- provisions of the Code should not have been 'a la carte' - CSPs should not have had the option to declare adherence to the Code only for specific personal data or specific services
- some kind of sign or logo should have been useful to make the decision easier for customers to choose between CSPs
- give some instruction or tools to the costumer to identify whether a CSP is a data processor (by default)
- monitoring or controlling by the costumer over data location needs further clarification.

4. Condition of adherence – process and relation to own T&Cs
5. Data Protection – substantive rights and obligations

5.1 Contractual specification – T&Cs

It was mentioned that:

- CSPs were not just data processors by default in practice (although it was covered by the Code)
- keep the text short and accessible - a separate explanatory document would be useful to give detail information on ambiguous issues (e.g. which qualify a CSP as a data controller)
- reference solely to the CSP without qualifying it as a data controller
- cross-references to SLA documents or work of the C-SIG SLA subgroup
- cross-reference to the work of other C-SIG Subgroups should have been outlined and explained
- Code of Conduct should have been the framing principle and not the SLA or a Service Contract.

5.2 Processing personal data lawfully

It was stated that:

- data processing by the CSP's own purposes would need further clarification
- last paragraph in this section set out main requirements on data retention by the CSP - there could have been a missing paragraph in this section on the customer's information about the level of retention because the CSP had to be instructed by the customer on the required level of retention
- statement of compliance (declaration of conformity??) would (should have) be(en) accompany the Code or could have been part of the Service Agreement - this short document would have contained company specific declarations on the CSP's conformity with relevant rules
- Code of Conduct would not overwrite the contract in any case.

5.3 Transfers within CSP's Group

It was mentioned that:

- considering data transfer between group members within a CSP Group different rules applied to each parties but the processing of data eventually was the costumer's responsibility
- default case in practice data transferred to a third party

5.4 Transfer to a third party

It was also agreed that

- third party issues such as subcontractors of the CSP should have been listed in the Code in two groups: (1) subcontractors within the group (third parties in parent-mother company relation with the CSP) by assessing the ownership of different parties and (2) subcontractors outside a CSP Group.
- statement of compliance could be also useful because the CSP is entitled to choose the location of the data
- keeping the list of subcontractors up to date (transparency) but business flexibility should also need to be taken account
- all subcontractors should have been listed with special regards to those who were not involved in the main data processing but processed data for minor data processing purposes
- costumer's consent to data transfer taking place within EU member states was not needed.

5.5 Right to Audit

It was also indicated that:

- data process should be cross-referenced to related issues in the SLA (references to the work of C-SIG SLA subgroup).
- it was not clarified in the Code who make the choice to proceed with the audit - some clarification is also needed to set out limitation if the audit was requested by the costumer.

5.6 Liability

It was indicated that

- a more detailed process considering the liability regime which was applied when the CSP failed to meet its legal obligations under applicable law (e.g. penalties etc.) should have been set out
- this section should be revised to meet these requirements.

5.7 Cooperation with customer

5.8 Data subject complaining

5.9 DPA request handling

5.10 Confidentiality obligations

5.11 Amendments to the Services Agreement

Considering changes in the list of subcontractors or in any other related issues concerning such subcontractors it was also mentioned that

- there was a difference if the subcontractor was situated within an EU member state or outside of the EU
- there was no need to seek the consent of the costumer if there were no substantial (organizational etc.) changes within the Group of CSPs
- this section of the Code should be clarified and tighten up this issue

5.12 Law enforcement requests

5.13 Data breaches

5.14 Termination of the Services Agreement

It was mentioned that

- telecommunication operators already had an obligation on data retention and deletion after the termination of the contract in line with the eCommerce Directive.
- SMEs did not have sufficient resources to comply with required processes in relation to the termination of the contract
- minimum set of requirements should have been outlined in this section
- costumers should be notified law enforcement public bodies submission to request to the CSP to have access to data - different rules applied in different jurisdictions
- in relation to data deletion the maximum time amount should be set out for CSPs as a general rule.
- some jurisdictions set out rules for CSPs to retain data for a longer period or it was needed for other reasons (e.g. backup etc.) - CSP had access to the data even after the termination of the contract
- such rules should have been inserted in an SLA
- SMEs did not have extended legal departments to tackle various requests in relation to the termination of the contracts thus a minimum set of requirements should have been set out in the Code - another solution to this problem could be an explanatory text linked to the confidentiality template.
- Code should not have been needed further additional parts, because it was more important to produce a user friendly, clear and short final document.

It was agreed that

- explanatory notes could have been placed in a background document (see also above explanatory document).

6. Security requirements – ensuring a baseline of good security practices

It was indicated that

- reference to standards in this section (e.g. ISO/IEC 27001) were too specific and it was more useful to refer to high level standardisation categories (requirements) - specific standards could be used as examples
- reference to Metaframeworks (current work of ENISA)
- basic security requirements were not set forth explicitly in the Code
- portability as a main concern was also mentioned.

7. Governance – management, application and revision, including bodies

As a general comment it was agreed

- current organisational structure in the Code was critical and too bureaucratic

It was also explained that:

- Governance section of the Code had not finalised yet.
- open call is envisaged to establish the governance in relation to the Code
- sustainable business model should have needed and the final structure was under consideration.

It was agreed that

- financial background for the envisaged governance model had not been finalised yet

- main aim was to have a Code that could be easily implemented and which was not so detailed
- marketing activities was also important.

7.2 Procedure for Self-Assessment by cloud providers

It was also indicated

- certification was preferable than a self-assessment by the CSPs itself
- Competent body's decision on self-assessment would not be well based if CSP's data centre would not have been visited.

7.3 Procedure for Certificates

It was indicated that

- in order to avoid duplication, cross-reference to the current work of ENISA on Metaframeworks instead of having a separate certification procedure.
- establishing risk categories for the audit.

Annexes

Transparency annex

Security objectives annex

It was detailed in a separate presentation below.

3. Security in the Code of Conduct

Nicolas Schifano gave a presentation on security issues regarding the CoC. Designated sub-subgroup of the C-SIG CoC Subgroup has dealt with the security requirements of the Code of Conduct as set out in Annex 1 of the document.

4. Further steps

Nicolas Dubois wrapped up the meeting and stated

- current version of the text was clearer in terms of scope and the text was more readable as well
- there would be two round of consultation with the SLA Subgroup before the text would be presented to the WP29 for endorsement
- comments to the text would be collected in a single document as well
- current stable version of the test would be circulated internally within the participants' organisation ('reality check')
- the text should have been circulated to DPA officers as well
- C-SIG Steering Board should have been the designated body who would present the text to the WP29
- deadline for the final comments should be received by the end of February in order to present the Code of Conduct to WP29 at the end of March.

5. Closing

Ken Ducatel thanked all participants for their contribution and closed the meeting at 17.30h.