DLAPvc20140214

Second follow-up VC on the non-EU/EEA Data protection Code of Conduct

Date	14th Feb 2014 at 16.05-17.10 CET
Participants	Patrick van Eecke, DLA Piper
	Valter Nordh, eduGAIN
	Mikael Linden, eduGAIN, notes

Community comments

Went through the comments 1.1-2.3 from the community that the DLA Piper memo by DLA Piper 29 Jul 2013 had risen.

- Unfortunately potential data importers' lawyers have provided no comments yet.

1.1. Why Standard Contractual Clauses?

More clarification why standard contractual clauses (SCC) approach (and not consent)

- As an alternative to the SCC, you could use consent, but it is cumbersome. You need to monitor and archive evidence of the consents given. Sometimes it is also cumbersome to get the consent from the user.
- In practice it is easier to just establish the SCC between the home organization and Service Provider

1.2. Data importer's ability to satisfy its legal obligations

SCC Annex 2, I(b) "It [i.e, the "data exporter"/Home Organisation] has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses."

- This is difficult.
- There are no guidelines or additional legislation to explain what a data exporter needs to do to “use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses”. There is no certainty how far you must go to do that.
- Some guidelines are available in Commission decision 2004/915/EC, item 5:
    - “the data exporter is also liable for not using reasonable efforts to determine that the data importer is able to satisfy its legal obligations under the clauses (culpa in eligendo) and the data subject can take action against the data exporter in this respect. The enforcement of clause I(b) of the new set of standard contractual clauses is of particular importance in this regard, in particular in connection with the possibility for the data exporter to carry out audits on the data importers’ premises or to request evidence of sufficient financial resources to fulfil its responsibilities.”
    - this suggest two alternatives
        - audits of the SP (which we thought would make SPs scared and decided to drop from the CoC)
        - request evidence of sufficient financial resources
    - the third alternative is to decide that the risk is low and can be taken
    - the duty can be passed to a third party (that’s what audits effectively are)

1.3. Liability and interference with other agreements

How does this interact with potentially existing Federation Agreements already covering the parties, specifically ruling out liability where possible (and limiting it to some rather low sum in all other cases, such as SWAMID's federation policy)?

- Draft 29 Jul 2013, 2.1: "this Charter applies without prejudice to the provisions as set forth in the

agreement between the Home Organisation and Service Provider which in all cases takes precedence over this Charter."

- the CoC is secondary to any other agreements (bilateral or multilateral, such as a federation agreement) so those take priority
- if HO and SP are not parties of a federation agreement (e.g. because they belong to separate federations), the CoC takes over

Does SCC leave room for HOs and SPs agreeing something else bilaterally?

- You can bilaterally agree to have some other legal basis than SCC, but that returns you to the starting point: you need to make the same exercise as we just doing in the CoC.
- There is a possibility to have another agreement on top of the SCC where the data exporter and importer can agree something else. Fore instance, there are cases where the exporter and importer have agreed that if the importer needs to pay for damages based on the SCC, the exporter will compensate that to the importer.
- Patrick would leave it up to the individual parties to agree something else bilaterally, on top of the CoC

1.5 Australia and adequate protection

The sentence on page 2 "The European Commission has so far recognised the following countries as providing adequate protection: Andorra, Argentina, Australia,..." caused confusion in the Australian colleagues.

- the sentence is a direct quotation from the EC website. It is indeed confusing.

2.3. Home Organisation's signaling their commitment to the CoC

Is it a strong enough signal of commitment to the CoC that a HO just decides to release attributes to an SP that has committed to the CoC?

- No, committing to the CoC by just releasing attributes to a CoC-committed SP isn't enough for a HO.
- The commitment must be an explicit act made by the home organization, at least an electronic signature.
- There is also the risk that a person that has configured the server to release attributes cannot make legal agreements binding the home organization.

Next steps

- Mikael goes through the DLA Piper draft and proposes changes (one week)
- Patrick checks the changes and provides the next version (one week)

Submitting the CoCs to WP29

- General data protection requlation status
  - estimate: finished before end of 2014.
  - then 2 year of adoption/grace period
  - the consistency mechanism that replaces WP29's approval for a Code of Conduct isn't available before the end of the adoption period
  - waiting until the regulation is effective is not an option for us
- Pros and cons of the WP29 submission
  - pros: WP29 approval would give much more power to the (two) CoC
  - cons: we will be challenged and confronted. WP29 is likely to ask us to change something
- GÉANT CoC and international CoC
  - Patrick proposes we approach WP29 only once
  - Either we submit only the GÉANT CoC to WP29 and don't submit the international CoC (because it just extends the GÉANT CoC to the SCC and the SCC is already a standard practice)
  - or submit both CoCs to the WP29 at the same time, in the same package
- It is up to us to make the decision
- useful reading for preparing WP29 submission:
  - WP29 procedure: Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct. Adopted on 10 September 1998 (pdf)
  - Example of an approved Code of Conduct: Federation of European Direct Marketing. European Code of Practice for the Use of Personal Data in Direct Marketing (pdf)