International Data Protection Code of Conduct drafts

Contents

Version 29 Jul 2013

DLA Piper draft (29 Jul 2013, for discussion purposes only)

- DLAPiper vc 13th Aug 2013
- DLAPiper vc 14th Feb 2014

1. Legal

1.1. (Peter) more clarification why standard contractual clauses (SCC) approach (and not consent)

- A: it is a well-known and widely-used catch-all apprach. See DLAPiper vc 13th Aug 2013 #1 and DLAPiper vc 13th Aug 2013 #2

1.2. (Peter) 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."

- Q: How this is done? What is sufficient? What kind of proof is needed?
- A: There are no guidelines or additional legislation to explain what a data exporter needs to do. However, the Commission decision 2004/915/EC suggests two alternatives: audit of the SP, or request evidence of sufficient financial resources from the SP
- Q: can this duty be passed to a third party (for scalability)? OTOH we have avoided making the federation liable
- A: yes (that’s what audits effectively are). See DLAPiper vc 14th Feb 2014

1.3. (Peter)Annex 2, III(a) liability

- Q: 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)?
- A: 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. See DLAPiper vc 14th Feb 2014
- Q: does SCC leave room for HOs and SPs agreeing something else bilaterally?
- A: you can agree something else but then you are not using the SCC. In some cases, the HO and SP can also have another agreement on top of the SCC where they agree something else. See DLAPiper vc 14th Feb 2014

1.4. (Olivier) Do the SP need to indicate its jurisdiction (in its metadata)

- A: Maybe. See DLAPiper vc 13th Aug 2013 #3

1.5. (Brook) 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 EC's adequacy decision covers only transfer of the passenger (PNR) records to the Australian Customs Service.

- A: The confusing sentence is a direct quotation from the EC website.

2.Organising

2.1. (Nicole) removal of GEANT’s role?

- A: Can be removed. See DLAPiper vc 13th Aug 2013 #5

2.2. (Nicole)What is legally strong enough to signal HO’s commitment to the iCoC?

- A: No ink-signatures needed? See DLAPiper vc 13th Aug 2013 #4

2.3. (Peter) Is it a strong enough signal of commitment to the CoC that the HO decides to release attributes to the CoC-SP

- A: 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. See DLAPiper vc 14th Feb 2014 #4

3. Technical

3.1. (inCommon) Consolidate the Code of Conduct spec in a single document

- A: Can be done if it is seen as beneficial. However, it is also possible that the two CoCs share some documents (e.g. the SAML2 metadata profile)

3.2. (inCommon) Standardize the Code of Conduct language that the SP must include in its Privacy Statement.

- A: Guidelines and a template is provided: Privacy policy guidelines for Service Providers

3.3. (inCommon) Avoid the use of <md:RequestedAttribute> elements in metadata to operationalize the Code of Conduct category. Consider using the attribute bundle approach instead.

- A: The idea in the CoC has been that there is no attribute bundle. The CoC can be used together with any set of requestedAttributes
- A: The CoC can potentially be used together with an EC that has an attribute bundle, such as R&S. A conservative interpretation of EU laws is that the attribute bundle is just an "upper bound" and you actually can release a subset of it.

3.4. (TomS) combine CoC and R&S entity categories in a way they can co-exist. An SP can assert both EC-with-bundle and CoC with RequestedAttributes. IdP decides which one of the two to use

- This approach may have potential. More planning needed

3.5. (TomS): EC-support attribute for CoC-IdPs?

- open issue: interference of parallel EC-support attributes is currently not well understood and requires wider discussion in the community
- open issue: Behaviour when a single IdP (hub&Spoke) represents several Home Organisations, potentially with different policies on which ECs they support