Data protection Code of Conduct (ver 18-11-2012), call for comments (closed on 31st Dec, 2012)
Resolution by the eduGAIN policy subtask, 19 February 2013
https://refeds.terena.org/index.php/Data_protection_coc

Abbreviation	Commentator's name	In which role the commentator have provided the comments
TL	Thomas Lenggenhager, SWITCH based on feedback from Esther Zysset, Legal Counsel of SWITCH	SWITCHaai Federation Operator
ML	Mikael Linden, CSC	Comments received during the Code of Conduct pilot with the CLARIN community
IY	Ian Young	Operations of the UK access management federation

Comments on the "GÉANT Data Protection Code of Conduct" document:

Ref		Section	Comment (justification for change)	Proposed change by the commentator	Resolution
CoC-1	TL	Lines 3-4	"European Economical Area" is wrong	Use "European Economic Area"	Accept.
CoC-2	TL	Lines 3-4	'countries with adequate data protection' is not specific enough	"countries with adequate data protection pursuant to [reference to relevant EU legislation]"	"…countries with adequate data protection pursuant to Article 25.6 of the directive 95/46/EC."
CoC-3	IY	Definitions	While IdP is defined as a *system component* (with "Home Organization" and "Agent" taking other roles), Service Provider is defined here only as an *organization*. For example, the entity category specification in this same document bundle uses "Service Provider" in the sense of the system component and it would be nice to have consistency to avoid possible misunderstandings.	Although as far as I can tell *this* document never uses Service Provider in its other sense as a system component, it might improve things for people reading this document in other contexts where that is the normal meaning of SP to use something like "Service Provider Organization" throughout in the CoC.	Reject change. There is indeed this conflict, but the term "Service Provider Organisation" is rarely used in our community and could cause confusion too, so the current approach is better. Usually the context indicates if we refer to the SP as an organization (obligations and rights and the legal stuff; this document) or technical component (SAML messages and other technical things; the metadata and Entity Category spec).
CoC-4	ML	2 e)	'e) [Data retention] to delete or	Add an explicit reminder that "the SP	Add the proposed reminder to the

			anonymise all Attributes as soon as they are not necessary any longer…' Many data controllers are not aware of the fact that they are not allowed to store user accounts forever if the user does not show up in the service.	must decide when the user accounts are deleted or anonymised if the user does not any more use the service".	Privacy Policy template.
CoC-5	IY	2 e)		"not necessary any longer" would be more colloquially worded as "no longer necessary"	Accept.
CoC-6	ML	2 f)	It is not necessarily clear for a reader that this clause applies when the service is actually provided collaboratively by several data controllers; for instance the SP triggers a Web Service which requires passing the Attributes further to another data controller	Add clarifying text to avoid misunderstandings.	Add "(such as a collaboration partner)"
CoC-7	TL	2 f)	On the basis of the general principle in 2 a), according to which Attributes shall only be processed in accordance with the relevant provisions of the applicable data protection law, it should be understood that attribute release to third parties on the basis of the third party committing to the Code of Conduct or similar (i.e. the second suggested alternative for attribute release) is only sufficient if this fulfills the criteria of the applicable data protection law. However, this is in our view insufficiently clear from the current proposed wording of paragraph 2 f).	"third party is committed to the Code of Conduct or has undertaken similar duties considered sufficient under the data protection law applicable to the Service Provider". As an alternative to such an add-on, we would welcome a reference to paragraph 2 a) on Legal Compliance with the applicable data protection law.	Accept
CoC-8	IY	2 i)	I don't understand what this sentence is saying, and in particular I don't know whether "which" is intended to refer to the updates, to the changes, or to the		Fix typo "any updates ***or*** changes in the local data protection legislation"

			local data protection legislation		
CoC-9	IY	2 j)	As a service provider, I would never sign up to do something "as soon as possible". It would imply that I would accept an obligation to take all steps possible to reduce the delay, even very expensive ones such as employing people 24x7x365.	A standard of "in a timely manner" or "without undue delay" seems more likely to be acceptable.	Replace “as soon as possible” by “without undue delay”
CoC-10	IY	2 j)	You are also missing any kind of constraint on the kind of breach which is to be reported. The current text reads as if the service provider accepts an obligation to report breaches and suspected breaches in *any* system, even one not related to the particular service. A suspected breach in the Service Provider organisation's payroll, or (even more extreme) in any other system in the world would appear to be covered by the current text but are presumably not intended. Again, as a service provider myself I would find it very difficult to agree to such an unbounded obligation, and in this case I'm sure you don't intend to impose one.		Add “privacy or security breaches (…) concerning the Attributes”
CoC-11	TL	2 j)	Three comments on the dropped part "including disclosure of Attributes to a law enforcement agency,...": 1) The issue of communication to a law enforcement agency is not strictly speaking an issue of security breaches and as such would merit a separate paragraph. 2) We consider that it makes sense		Reject. The comment is valid but follows already from the law. Here we would like to keep the CoC as simple as possible.

			to put this back in for cases where disclosure of the ordered information is not subject to a prohibition by the law enforcement agency. If necessary, the following could be added: "including disclosure of Attributes towards a law enforcement agency to the extent possible". 3) We consider it would make sense to add an additional phrase to that paragraph stating that the Service Provider undertakes to only disclose information to law enforcement agencies upon issuance of the relevant orders or warrants as required by the applicable law. The reason for this being that although such warrants or orders are generally required for disclosure of information to law enforcement agencies, there is a tendency amongst companies to give in to such requests on the basis of informal requests, whereas privacy and data security are enhanced for the end user if the SP insists on compliance with such formal requirements.		
CoC-12	TL	2 k)	Taking the point of view of an SP, the vagueness of 2k) [Audits] makes us very uneasy due to limitless costs and effort	Specify who nominates the "independent and specialised third party"	Drop clause 2k) [Audits] to make the Code of Conduct less scary for SPs.

			required provided PWC would show up on or door step to make an audit of the SP! Who nominates the "independent and specialised third party"? The SP admin himself? The 'to permit periodic audits' leaves it open who pays for it, so it might also be the SP. The effort to support an audit (even paid for by a third party) might still consume quite some effort. This makes us uneasy to accept such a vague statement. The effort and costs for the SP need to be reasonable. I do agree that it would be good to have the principle of the SP submitting to audits. However, our concern was that this is somewhat broad and that it might scare off SPs. So, in consequence, in my view it might be worth specifying more (who appoints the auditor, who pays) or limiting the language (for instance by specifying that they audits are carried out max. on an annual basis).		The General data protection regulation, when effective, may introduce a common practice for audits. The proposed version (Article 22.3) imposes the obligation to the SP: “The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.”
CoC-13	TL	2 l)	The current 'to hold harmless...' is great for the End User and the IdP or its Agent, but is very frightening to an SP since it is without any limits. You generally limit the liability to something which satisfies both sides. We think it makes this item easier to accept for the SP if we add that	Add “…as determined in a binding and enforceable judicial ruling”	Accept

			the holding harmless by SP requires a judicial ruling. This requirement is not unreasonable, since most likely the SP would anyhow not just accept any bill presented by the IdP or End User.		
CoC-14	TL	2 m)	"transferred outside the European Economic Area," is not sufficient. "and countries with adequate data protection pursuant to [reference to relevant EU legislation]" is missing	Reuse the same reference in lines 3-4.	Accept
CoC-15	TL	2 m)	We propose a simplification of the text because the previous text would not have covered the countries outside EEA but within the set of countries with adequate data protection. The text deleted is implicit when mentioning 'the law of the country in which the Service Provider is established'.	Replace “articles 25 and 26 of the EU directive 1995/46/EC, as transposed in the national ” by “the”.	Accept
CoC-16	TL	2 m) & 2 n)	"Service Provider has been established," & "Service Provider is established;"	Resolve the inconsistency	Use “is established”
CoC-17	TL	2 p) b	"termination of the service provision to the Home Organisation;"	"termination of the service provisioning to the Home Organisation;"	Accept