GÉANT data protection Code of Conduct comment form
https://refeds.terena.org/index.php/Code_of_Conduct_for_Service_Providers

Please fill in and submit by e-mail to `edugain-policy-comments@geant.net` no later than on the 12th of August, 2012. Received comments and related resolutions will be published.

Commentator's name and contacts	Paul Millar <paul.millar@desy.de>
In which role you have provided the comments	As technology provider (dCache) with an interest in federated identity

In general,

☐ I am/we are comfortable with the Service Provider Code of Conduct

☐ I am/we are comfortable with the Service Provider Code of Conduct, our comments below are taken into account

☐ I am/we are not comfortable with the approach (please propose an alternative approach with reasoning).

Specific comments:

Line(s)	Comment (justification for change)	Proposed change by the commentator	Resolution by REFEDS/eduGAIN workgroup
33	"Legal compliance" seems unnecessary: does an organisation need to assert that they will be lawful?	Remove a)	
34,78,81	The question of which country's Personal Data protection law(s) the SP is bound may not always be easy to express; for example, if a service is distributed over multiple countries or is a federated service.	Remove explicit definition of which country's law is in effect [n) and references in a), m)]. Instead, add a requirement in h) that the Privacy Policy includes a statement of which country has jusitiction, who's data-protection laws are in effect, etc	
38	"least intrusive Attributes" is	Provide some guideline on how	

	ambugious: what defines intrusiveness? For whom is the test applied (End User, Home Organisation, IdP, SP, Agent, …)?	“intrusive” is determined and against whom it is tested.	
36,41,46	The phrase “enabling access” appears multiple times in the document. There may be uses for attributes outside of simply enabling access; for example, if a service logs activity (often a legal requirement) then this log may contain attibutes, yet this is not “enabling access” (except through some tortuous logic)	Consider using a better phrase.	
42	The clause “prior consent has been given [..] End User”. From talking to others in FedId community, I've heard that this can be a contentous point for some IdPs.	Give serious consideration to removing the “consent from End User” clause. It isn't needed if agreement is reached via Home Organization [see clause s)]	
43	Anonymising is both difficult to achieve and has a poor track record as a mechanism to protect individuals' Personal Data.	Consider stipulating only “delete”.	
44	“processing activity” is vague: what is an “activity”? What does it mean to “process” it?	Use more careful language in describing what is allowed.	
45	Again, there is the potential problem with obtaining prior consent.	Give serious consideration to removing the prior consent clause.	
45	A SP may be required, under law, to disclose attributes to law agencies. This possibility isn't covered by f)	Add a statement about disclosure required under law.	
52	Privacy policy seems to be missing some important information: 1. under what circumstances can the Privacy Policy change? 2. What notification (if any) will the End User get that the policy has changed	Add information that the Privacy Policy must describe how it can evolve over time.	

	3. Where can the End User obtain the latest version of the Privacy Policy		
57-59	Items d. and e. seem to overlap: any transfer to a country outside EEA is necessarily a 3rd-party recipient.	Consider merging these two items	
52	Provide to the End User … the assumes that the service is provide in a mechanism that permits this (e.g., via a web portal). It is possible to use federated identities through non-web services (e.g., Project MoonShot).	Perhaps rephase “at least at first contant” as “at least on or before first contact with the service” or add a get-out-clause (e.g., if technologically possible), although I don't like the second option.	
68	“to immediately report” When an SP has been hacked or otherwise suffered a breach, the immediate response may be to secure the service, preserve evidence and understand the damage.	First, suggest replacing “immediately” with something that expresses the same urgency but that allows the possibiliity of other actions taking priority (e.g., “as soon as possible”).	
70	If a site has provided information to a law enforcement agency then they may be under a legal compulsion not to reveal this.	A statement that the SP will make every effort to inform the End User of any disclosure (or similar) – e.g., they will only keep the information hidden if legally compelled to do so. (even then, they could challenge this).	
72	“Permit period audits” this clause seems problematic: • who is permitted access to the attributes: the SP, an external auditor, the Home Organization, the End User? • The scope of the audit is missing some attribute activities (e.g., storage of and transfer of attributes)	Suggest rephrasing the clause to make certain points clearer.	

	• Wouldn't an external audit consititute a disclosure of attributes, which goes against cause d) and f). This suggests the audit is internal (i.e., within the SP). • What is the result of an Audit? What does the SP promise to do with the report?		
88-91	Clauses p) and q) seem somewhat at odds: if the adherence of the CoC is terminated, how is there any expectation that clauses are honoured?	I'm not sure what to suggest here: the sentiment is fine. Perhaps there needs to be some action taken by the SP on exiting the agreement (e.g., delete all attributes).	
89	The CoC states “the agreement” without defining it: is this an agreement between the End User and the SP, between the Home Organisation and the SP or some other agreement?	Suggest tightening up the language about which agreement and between whom.	
89	The CoC states “the Home Organisation”; however, an SP will likely accept attributes from many IdPs. Must all agreements be terminated to terminate adherence to the CoC or just one. If one, which one.	Suggest tightening up the language describing “the Home Organisation”	
92	The process of updating the Code of Conduct seem very vague. Who decides if an update is minor or major? Who can propose a minor or major update? Who must agree before a minor or major update is binding? Who is notified if there is a minor or major update?	Suggest making this process clearer	