Code of Conduct Consultation

This consultation is now CLOSED

Background

A Code of Conduct to support compliance with data protection regulations has been available for sometime (https://geant3plus.archive.geant.net/Pages/uri/V1.html) but is out of date as it references the old Data Protection Directive and not GDPR. A version 2 has been in progress for a number of years and has been consulted on with the community several times (see Historical / project information). It had been hoped that this would be published as a formal European Data Protection Board (EDPB) approved Code as described in Article 40 of GDPR. After several efforts, the team supporting CoCo concluded that it was sadly not possible to achieve this aim (see: https://refeds.org/a/2577).

It is now proposed that the Code be published as a Best Practice document to allow Service Providers to signal their compliance with data protection regulations without taking the form of a ratified code. Since the last consultation, the documents have been simplified to meet the best practice statement as some elements required in the formal code are no longer necessary. It has also been proposed that the new CoCo be published as a REFEDS specification to ensure its long-term sustainability.

The new Code of Conduct is addressed to:

- Service Provider Organisations established in any of the Member States of the European Union and in any other countries belonging to the European Economic Area (Iceland, Liechtenstein and Norway).
- Service Provider Organisations established in any third country or International organization offering an **adequate level of data protection** in the terms of Article 45 of the GDPR or **appropriate safeguards** in the terms of the Article 46 of the GDPR can also subscribe to this Code of Conduct.

Overview

This consultation will be open from **12th November 2021** at 17:00 CET and will close on **10th December 2021** at 17:00 CET.

Participants are invited to:

- to consider the proposed entity category.
- to consider the proposed Best Practice document.
- propose appropriate changes / challenges to the proposed text in both documents, and
- confirm that they are happy that this should be considered as a REFEDS Entity Category and Best Practice document.

The document for the consultation is available as a pdf attachment (entity category) and pdf attachment (best practice). All comments should be made on: consultations@lists.refeds.org or added to the changelog below. Comments posted to other lists will not be included in the consultation review.

Change Log

comment #	Line /Reference # (please indicate which document is referenced too - e.g. EC line 1, BP line 1)	Proposed Change or Query	Proposer / Affiliation	Action
1	6	I find the opening line a little confusing since the service provider may choose to commit to more rules than just the ones in this framework. "This Code of Conduct sets the rules that Service Provider Organisations can commit to when they..." -> I would suggest a slight change to "This Code of Conduct defines a set of rules that…"	Hannah Short /CERN	Accepted.
2	General	Since the Code of Conduct is really about expressing compliance with GDPR I wonder whether the title of the entity category and framework shouldn't be clearer and refer to the fact that it's about GDPR and not a more general Code of Conduct? Peter: Well, it's the "**Data Protection** Code of Conduct" in both cases (so clear enough, I think). While v1 was specific to 95/46/EC it wasn't called the "EU Data Protection Regulation" Code of Conduct and I wouldn't make v2 the "GDPR Code of Conduct" either. I do recall it was previously suggested to add "for Identity Federation" at the end (or something along those lines), though.	Hannah Short /CERN	Rejected. We concluded an explicit reference to GDPR in the title would give a false impression that this Code of Conduct is approved by the authorities. However, “data protection” in general refers to the European data protection laws

3	EC - 80	"the registrar MUST at least: ... 7. Ensure **they** have an appropriate administrative contact that is aware of the Service Provider's commitment to the Code of Conduct." "they" points to the registrar. Is it the intent the registrar has an administrative contact?	Niels van Dijk (SURF)	Accepted. Replaced "they" by "the Service Provider"
4	EC - 66/77	What if the "check" fails? What is the difference between "ensure" and "check"?	Niels van Dijk (SURF)	Accepted. Reformatted the bullet list
5	EC 62	Does a RA have the right to revoke registration? If so should that be mention in the document?	Niels van Dijk (SURF)	Accepted. Added a sentence to the end of the section "The Registrar has the right to remove the Entity Category if the Service Provider can no longer demonstrate commitment to the REFEDS Data Protection Code of Conduct [CoCo]"
6	EC 74	Explicitly reference chapter 5 here?	Niels van Dijk (SURF)	Accepted.
7	EC 74/77/87	If registration criteria #3 already mandates accordance with 5.5.1, why is registration criteria #5 still needed?	Niels van Dijk (SURF)	Accepted. Removed #5.
8	EC 93/94	MUST clause in 5.1.4 , why? If the entity is only for intrafederation use , eg only Spain or Germany then why put such a clause? maybe MUST is required if exported into eduGAIN ?	Alan Buxey /independent	Rejected. English is important (even in a national setup) to make sure all data subjects are informed and know how to use their rights. Requiring at least English is also consistent with the eduGAIN SAML2 profile.
9	EC 85	Do we also need a metadata requirement for the Registrar/federation? - their tooling needs to support this entity category	Alan Buxey /independent	Rejected. REFEDS has currently no ECs with metadata requirements for the Registrar.
10	EC 98	Theres an implementation clash with CoCo and entity category attribute bundles (eg R&S) - the best practice states data minimisation and only request what you need (BP 134) but R&S and other authorization entity categories have values that may be optional. This section in EC states that 'RequestedAttribute' MUST be used for those required - suggesting theres an implementation required that if such values exist and CoCov2 asserted then a CoCo IdP should ignore the R&S and only release the values requested..... IdPs in other jurisdictions or that do not follow CoCo just honour the R&S . if so, this should be explicitly stated.	Alan Buxey /independent	Rejected. The REFEDS view has been that if there are several ECs the IdPs shall interpret them in parallel and independently.
11	General comment for EC and BP	It is understood that it is not mandatory to assert or fulfil this EC, and it is understood that information is provided at a national level (and therefore this information will be made available to the SP nationally) but perhaps it would be a good opportunity to include within the best practice additional information the benefits of asserting and fulfilling CoCo, and the implications of not doing so	Michelle Williams (GEANT)	Rejected. There is already a sentence of CoCo's benefits ("Home Organisations will feel more comfortable to release…") both in the beginning of the BP and the EC. Additional promotional material will be provided separately.
12	EC - General	Should it clearly state that v1 is to be deprecated and refer to the fact that it is up to each federation to annouce its intended timelines for deprecation? Should it also position the fact that the national federation will define the rules for the transition?	Michelle Williams (GEANT)	Rejected. CoCo v2 is not the proper place to define the deprecation of v1. Deprecation of v1 needs to be managed and communicated separately.

13	EC - General	There is no clear guidance on the rules and the subsequent consequences of how 3rd countries outside the EU/3rd countries with adequacy agreements should behave. That is, as an SP in a 3rd country is not entitled to assert CoCo, what are the consequencies if, for example, the services becomes the subject of the 3rd country (via a company takeover or IT outsourcing decision) subsequent to initial registration? It is understood that it's the RA asserting the EC at the request of the SP, and that checks will be made at the point of registration, however it's not clear what the ongoing mandatory commitments of the SP are, i.e., that they must continue to demonstrably fulfil the requirements of CoCo or the SP must immediately inform the RA in the event that they no longer fulfil the requirements.	Michelle Williams (GEANT)	Accepted. Added a new bullet point “In possessing the Entity Category Attribute with the above value, a Service Provider claims … that it informs the Registrar about any material changes that may influence their ability to commit to the REFEDS Data Protection Code of Conduct [CoCo].”
14	EC - 23-25	There is no explicit statement that confirms that SPs outside this scope are not entitled to apply to assert CoCo	Michelle Williams (GEANT)	Rejected. Lines 23-25 make it clear who are in the scope of the CoCo. The rest are out of scope.
15	EC - L43 - 47	There is no explicit description of how changes to the use of the data subsequent to its original registration might impact the SP's right to assert CoCo in the future. i.e., the SP might be in scope for CoCo when the SP is registered, but the business might change after registration to the point where the SP no longer meets the requirements for CoCo. How does a SP or RA ensure that it still complies to the requirements of CoCo, and what obligations do the parties have to ensure that is the case? The RA commits to checking at registration, but commits to subset of regular checks, perhaps it could be made clearer that it is the SP's responsbility to ensure that it continues to comply and that it is the SP's responsibility to flag if they no longer comply.	Michelle Williams (GEANT)	Accepted – See #13.
16	EC - L54	Should explicitly state v2?	Michelle Williams (GEANT)	Refined the reference – REFEDS Data protection Code of Conduct [CoCo] and [CoCo] describes the exact document.
17	EC - L59-61	Should it be made clearer here (or in the best practice) that an IdP isn't bound or obliged to release the requested attributes?	Michelle Williams (GEANT)	Rejected. This question was discussed extensively in the Personalised EC work and the conclusion was copied here.
18	BP - L72	‘can commit to’ – should be must (I can, but I choose not to) – ‘the measures that the service has employed and commits to’	Michelle Williams (GEANT)	Rejected. This is just an introductory paragraph. Later in section Principles for processing of attributes the Service Provider Organisation “agrees and warrants…”
19	BP L117-119	if I understand the intent correctly, it might be better to simply state “Service Provider Organisations may manage and register several independent Services, however, those doing so are asked to commit to the Code of Conduct for each Service separately”	Michelle Williams (GEANT)	Accepted.
20	BP L134-136	How is ‘access to the service’ defined?	Michelle Williams (GEANT)	There is a wide range of different services and access may mean different things for them. Want to leave a broad interpretation of the expression.
21	BP L205-206 and Section O	There is no effect of termination in the event of c. i.e., the SP should request removal of the EC, but it’s not set out here or in 524-532; options for termination are not useful if there is no explicit effect of that termination	Michelle Williams (GEANT)	Accepted. Added a new paragraph to the end of section 4 in the EC specification: “The Registrar has the right to remove the Entity Category if the Service Provider can no longer demonstrate commitment to the REFEDS Data Protection Code of Conduct [CoCo].”
22	BP L301	remove ‘is’ at end of line	Michelle Williams (GEANT)	Accepted.

23	BP General	The effects of non compliance aren't explicitly clear	Michelle Williams (GEANT)	Accepted. See #5.
24	BP Section F	Quite possibly too descriptive: without understanding the nuances of the service's use of PII, it might not be advisable to make statements that paraphrase an understanding or perspective of the regulations; perhaps only the relevant sections of the regulations should be referred to here?	Michelle Williams (GEANT)	Accepted. Replaced strict 18 month retention time by “it is considered as a good practice to delete or anonymise the End User’s personal data if they have not logged in for a significant period of time”
25	BP Section J	Standard contract clauses' should be 'Standard Contract Clauses' and a reference should be provided.	Michelle Williams (GEANT)	Accepted.
26	BP Section L	Perhaps this should instead refer to all parties holding the authors of the Best Practice harmless? GDPR has specified liaibilities that might be dangerous to paraphrase here	Michelle Williams (GEANT)	Rejected. Because of the liabilities this sentence was developed by the legal advisers.
27	EC section 5.2.1	If the SP conforms to the subject identifier profile, then it has to signal the requirements as per the profile, so it's arguable that the section is extraneous. However, you obviously want to say something about subject identifiers (as they're personal data, after all). Note also that the text itself is somewhat confusing 1) an SP can conform to the profile and signal that it does not require a subject identifier, so it can't indicate which one of the identifiers is necessary, because neither may be 2) how you refer to the entity attribute isn't clear. Therefore, I think the section needs a rewrite.	Alex Stuart (Jisc)	Accepted. Added a clarifying paragraph.