2021 Position: GÉANT Code of Conduct version 2

Background

Since 2014, the GN4 project has been looking to revise the existing Code of Conduct for Service Providers using identity federations. This has become necessary for range of reasons:

- The introduction of GDPR, rendering the current CoCo, which is tied to the Data Protection Directive (directive 95/46/EC) obsolete.
- The desire to extend CoCo beyond the boundaries of Europe.
- The more detailed and official process for creating and approving Codes of Conduct introduced in the GDPR.

An approval of the GÉANT CoCo would be done by the European Data Protection Board (EDPB) and, according to GDPR, would:

- contribute to a controller demonstrating proper information security (Art 24, 28, 32).
- contribute to a controller's the Data Protection Impact Assessment (Art 35).
- enable international transfers for controllers (Art 46). However, EDPB's guidelines on codes of conduct for international transfers are still pending.

This paper outlines issues that have been identified as the process for registering Codes of Conduct has become clearer, as new advice has been issued and as part of initial discussions with the Dutch Data Protection Authority (DPA).

Identified Issues:

1. **Separate EU and International Codes**

In the meeting with the GÉANT team in January 2020, the Dutch DPA underlined that it understands our approach to have a single code of conduct covering all purposes. However, it believes that it will be too complex to deal with both intra-EU processing of personal data and international transfers of personal data within a single code of conduct, in particular given that the guidelines on codes of conduct as a tool for international transfers are still being discussed within the EDPB and are not expected soon.

Thus, the Dutch DPA recommended us to focus at this stage on a clear framework for intra-EU processing of personal data and to leave aside international transfers.

This would thus entail that we remove all aspects related to international transfers of personal data and exclude adherence to the Code of Conduct by Service Providers based outside of the EU (including International Organisations).

The value of this approach is currently very uncertain. The draft of the current proposed Code of Conduct v2 is lengthy and focused, and this was strongly driven by a desire to achieve a unified, global approach to the Code. It is also very questionable as to whether an

intra-Europe code has much value, given it is not one of the core 6 principles for processing identified in Article 6 of the GDPR: https://gdpr-info.eu/art-6-gdpr/. A non-EU focus would perhaps make more sense, but this was not the recommendation received from the DPA.

2. **Monitoring Body: Independence**

The European Data Protection Board (EDPB) has provided some guidelines on how the expect DPA's to implement support for Codes of Conduct and accreditation of monitoring bodies:
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en.

These guidelines set a high bar for independence that it would be difficult for GÉANT to meet as a membership organisation. The funding mechanisms of the GN4 project could also impact perceived independence. This means it would be highly likely that an alternative body or organisation would need to be found and the way in which CoCo work is funded would need to be reconsidered.

Some consideration to alternative hosts (e.g. not GÉANT) has been given. Potential hosts considered have been REFEDS, Kantara or Scope Europe (https://scope-europe.eu/en/monitoring-body.html). Use of an external body would raise questions regarding funding model and whether the organisation is happy to take on liability.

3. **Monitoring Body: Liability**

The GDPR holds the monitoring body full liable for infringements by users of the Code.

If the monitoring body fails to (Art 41.4) *take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code* the monitoring body is (Art 83.4) *subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.*

This could mean that the Monitoring Body could be if it is not able to demonstrate that it has properly fulfilled its obligations. In the eduGAIN context, this would mean GÉANT would take on liability for organisations well outside its membership if it took on the Monitoring Body role. This would mean the monitoring body would need to be funded and staffed at a level that would mitigate this risk.

The GÉANT Code of Conduct can currently be used by any federation and can therefore appear in parameters that are not technically monitored by eduGAIN. There are NREN federations and other communities (e.g. EGI) who have shown interest in integrating the GEANT CoCo also to their local/community policy frameworks.

It is unclear if such liabilities could be mitigated by insurance.

4. Monitoring Body: extensiveness of checks

CoCo already has a well-defined mechanism for checking technical compliance with CoCo v1 and this could be easily replicated for CoCo v2. At the moment, however, there is no strict follow up on resolving identified issues and this is broadly left to the entity owner. In order to meet the monitoring requirements identified by the EDPB and manage the risks associated with the liability for the Monitoring Body, significant proactive and reactive work would be needed to ensure compliance and risk management. This would add to the costs of providing such a service significantly. New approaches to ensuring CoCo is removed from non-compliant entities would need to be put in place.

5. Current Options

The following options have been identified for how to resolve the current position with the Code of Conduct. In consultation with the community, there was a clear desire within the community to continue to find a path to have a way of indicating compliance with data protection guidelines within metadata.

Funding for any of the options remains an issue - the available funds for legal support within GN4 have already been used and the potential costs for running a monitoring body and dealing with liability have yet to be fully articulated.

	Option	Issues	Decision
1	Do nothing	As CoCo v1 is currently obsolete due to its references to the deprecated Directive, this is not an option. A decision on whether to properly deprecate CoCo v1 or continue with one of the other options in this list.	This is not an option, action is needed even if this means only deprecating v1.
2	Establish CoCov2 as a Best Practice Guide rather than a formally ratified Code and deprecate v1.	The second option could be to make some amendments to CoCo v2 to operate as a best practice approach. This has some benefits in being very lightweight (privacy statement plus entity category) compared to the demands of a fully ratified Code.	This is currently the preferred approach pending further ratification.
3	Continue with CoCo version 2 for Europe (plus	As indicated in section 1 above, there is limited	There is still a strong motivation to pursue a

	those with an adequacy decision?)	value in a Code for Europe only when balanced against the expense of the requirements outlined and other options available to providers and institutions via the standard six principles for data transfer. The monitoring body costs, liability and independence issues would still need to be addressed in this scenario.	recognised EDPB ratified Code of Conduct, however there are a number of issues that need to be resolved before moving forward, some internal, and some in relation to the DPA. Overall, the preference is to avoid having separate Codes of Conduct for Europe and third-party transfers as this will create implementation barriers. If we want to pursue that line, we will need to wait until the EDPB and the Dutch DPA are in a better position to give advice on third party transfers.
4	Continue with CoCo version 2 for third country transfers only	As the Code of Conduct mechanism is presented in the GDPR as a solution for third country transfers this option would seem to make more direct sense than pursuing a code for intra-Europe transfers and would support a clear problem area - given user consent (which is problematic) and contractual approaches are currently the only mechanisms for third country transfers. The benefits of this to GN4 members would need to be clearly demonstrated, but the breadth of international transfer in research and education projects can easily demonstrate this need. The monitoring body costs, liability and independence issues would still need to be addressed in this scenario.	
5	Continue with CoCo	This position would mean	

	version 2 for intra-Europe and third country transfers	pushing back against the recommendations from the Dutch DPA and asking them to reconsider based on the environment that we operate in, where separate Codes make little sense to international research. Continued legal support would be required in this scenario. The monitoring body costs, liability and independence issues would still need to be addressed in this scenario	
6	Diversify CoCo version 2 to two service levels for different service providers	This combines #4-#6 (approved CoCo) and #3 (CoCo as a best practice). The high-end service providers (who are willing to pay for receiving attributes) commit to a "CoCo Gold" that seeks an approval by the Dutch DPA, has a monitoring body and an annual fee that covers the monitoring costs. The low-end service providers would commit to "CoCo Silver" which is a GEANT best practice (similar to CoCo1 now). Gold's and Silver's requirements for an SP would be materially the same but Silver has no monitoring body and fee. An IdP can decide attribute release to Gold and Silver SPs independently.	This option is regarded as overly complex and would not support adoption at the rate needed.

6. Next Steps

At the current moment in time, work on the GÉANT Code of Conduct is currently on pause for a variety of reasons. The following issues should be resolved in order to make an appropriate decision about next steps.

- **Immediate funding**: there is no more funding available for legal advice for this work. If we wish to continue using external legal advice, additional funding would need to be secured.
- **Future funding**: thought should be given to the funding model for running a monitoring body in the future scenarios laid out above.
- **Liability**: advice on whether it is possible to secure insurance for liabilities incurred under GDPR fines as a monitoring body is needed.
- **GÉANT position**: a firm statement from GÉANT as to whether it considers its role as a monitoring body for CoCo to be tenable should be sought.
- **Alternative bodies**: further work should be undertaken to review the viability of alternative monitoring bodies and their position on funding, independence and liability.
- **CoCo v1**: a position on CoCov1 and whether this should continue to be supported or deprecated should be taken.