GÉANT Code of Conduct

To address data protection issues in Europe

SWITCH

Thomas Lenggenhager
aai@switch.ch

Interfederation Crash Course
Bern, 1. March 2013

GÉANT Data Protection Code of Conduct

- Full title of the GÉANT CoC:
  - GÉANT Data Protection Code of Conduct for Service Providers in EU/EEA
  - It is still in draft status
    - https://refeds.terena.org/index.php/Code_of_Conduct_for_Service_Providers

- The GÉANT CoC is expected to satisfy the data protection issues for parties within:
  - European Union
  - European Economic Area
  - countries with adequate data protection pursuant to Article 25.6 of the directive 95/46/EC
    - e.g. Switzerland

- During GN3+, the concept of CoC should get enhanced to also cover SPs in any other countries

GÉANT Data Protection Code of Conduct (2)

- With the CoC, SPs confirm that they adhere to the rules listed in it
  - It is mostly what is anyhow required by national law or best practices, just explicitly listed in a single document
  - Specific requirement to provide a link to the SP's **Privacy Policy** that includes:
    a) the name, address and jurisdiction of the Service Provider;
    b) the purpose or purposes of the processing of the Attributes;
    c) a description of the Attributes being processed;
    d) the third party recipients or categories of third party recipient to whom the Attributes might be disclosed, and proposed transfers of Attributes to countries outside of the European Economic Area;
    e) the existence of the rights to access, rectify and delete the Attributes held about the End User;
    f) the retention period of the Attributes;
    g) a reference to the GÉANT Code of Conduct;

→The Resource Registry already allows you to add a Privacy Policy URL for an SP

GÉANT Data Protection Code of Conduct (3)

- SP's confirmation to be included in the SP's metadata as an Entity Category attribute, e.g.:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="https://service.example.com/entity">
  <Extensions>
    <EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="http://macedir.org/entity-category">
        <AttributeValue>
          http://www.edugain.org/dataprotection/coc-eu-01-draft
        </AttributeValue>
      </Attribute>
    </EntityAttributes>
  </Extensions>
   ...
</EntityDescriptor>
```

GÉANT Data Protection Code of Conduct (4)

- It is expected that
  - the CoC makes IdPs more comfortable to decide to release attributes to SPs from other federations
  - IdPs will choose to release certain attributes only to SPs that have a CoC Entity Category attribute in metadata

- The CoC is one of the means for federations without a scalable attribute release to support scaling for interfederation
  - SWITCHaai supports default attribute release policy and tailored `attribute-filter.xml` files.

- SWITCH will keep you up-to-date about developments in the area of CoC.