

Recipe for a Service Provider

The Data protection Code of Conduct (CoCo) enables safe attribute release between Identity and Service Providers within EU.

The following steps explain how to support the Code Of Conduct for a Service Provider.

1. Read and understand the GEANT Data protection Code of Conduct for SPs:
 - [GÉANT Data Protection Code of Conduct for Service Providers](#)
 - For a more complete presentation of the Code of Conduct, please have a look at [TNC2013 Code of Conduct Presentation](#) or [the memorandum](#) prepared for Article 29 working party
2. SP's jurisdiction:
 - Is the SP established in EU/EEA, or in a country/jurisdiction with adequate data protection ([the EC white-list](#))?
 - The GEANT Data protection Code of Conduct for SPs in EU/EEA is only applicable for those SPs
3. Find out if the organization that is responsible for the SP feels comfortable to commit to the GEANT data protection Code of Conduct for SPs:
 - As an SP administrator, you may need to ask someone above you in your organization
 - Remember: In many cases there is nothing to worry about because in EU/EEA countries, many of the CoCo requirements are already mandated by the data protection laws
4. Develop a list of attributes that are necessary for enabling access to the service:
 - See [What attributes are relevant for a Service Provider](#)
5. Provide a name and description for the service:
 - There must be at least an English name and description
 - Choose names that are meaningful for the end user who might not be familiar yet with the service
 - Good example:
 - Name: University of Tübingen's Weblicht tool for linguistics research
 - Description: WebLicht is a chaining tool for linguistics research. It provides an execution environment for automatic annotation of text corpora.
 - Bad example:
 - Name: Finna
 - Description: Public Interface Finna.
6. Develop and publish a Privacy policy document:
 - It must contain a link to the GÉANT Data Protection Code of Conduct: <http://www.geant.net/uri/dataprotection-code-of-conduct/v1>
 - There must be at least an English version available:
 - It is recommended to write the document using this template: [Privacy Policy Guidelines for Service Providers](#)
7. Ensure that the Service Provider is registered in your federation/eduGAIN with the following SAML2 metadata elements:
 - Entity Category attribute for the Code of Conduct
 - mdui:PrivacyStatementURL
 - list of md:RequestedAttributes
 - mdui:Displayname (recommended)
 - mdui:Description (recommended)
 - For details of these elements, see [SAML 2.0 profile for the Code of Conduct](#)
 - How these elements are registered depends on your local federation
 - Find below an example of how the metadata looks like for a Service Provider that supports the GEANT Code Of Conduct.

```

<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://filesender.example.org/">
  <Extensions>
    <EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
        Name="http://macedir.org/entity-category"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</AttributeValue>
      </Attribute>
    </EntityAttributes>
  </Extensions>
  <SPSSODescriptor>
    <Extensions>
      <UIInfo xmlns="urn:oasis:names:tc:SAML:metadata:ui">
        <!-- At minimum an English display name and a description -->
        <DisplayName xml:lang="fi">FileSender</DisplayName>
        <DisplayName xml:lang="en">FileSender</DisplayName>
        <Description xml:lang="fi">FileSender tarjoaa helpoa tavan jakaa suuria tiedostoja.</Description>
        <Description xml:lang="en">FileSender offers an easy way to share large files with anyone.</Description>
        <!-- This URL must contain a privacy statement that must include a link to the GEANT Code of Conduct
        (http://www.geant.net/uri/dataprotection-code-of-conduct/v1) -->
        <PrivacyStatementURL xml:lang="fi">https://filesender.example.org/privacy-fi.html</PrivacyStatementURL>
        <PrivacyStatementURL xml:lang="en">https://filesender.example.org/privacy-en.html</PrivacyStatementURL>
      </UIInfo>
    </Extensions>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
https://filesender.example.org/saml/acs" index="1"/>
    <AttributeConsumingService>
      <RequestedAttribute
        FriendlyName="displayName"
        Name="urn:oid:2.16.840.1.113730.3.1.241"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        isRequired="true"/>
      <RequestedAttribute
        FriendlyName="eduPersonPrincipalName"
        Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        isRequired="true"/>
      <RequestedAttribute
        FriendlyName="mail"
        Name="urn:oid:0.9.2342.19200300.100.1.3"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        isRequired="true"/>
    </AttributeConsumingService>
  </SPSSODescriptor>
</EntityDescriptor>

```