

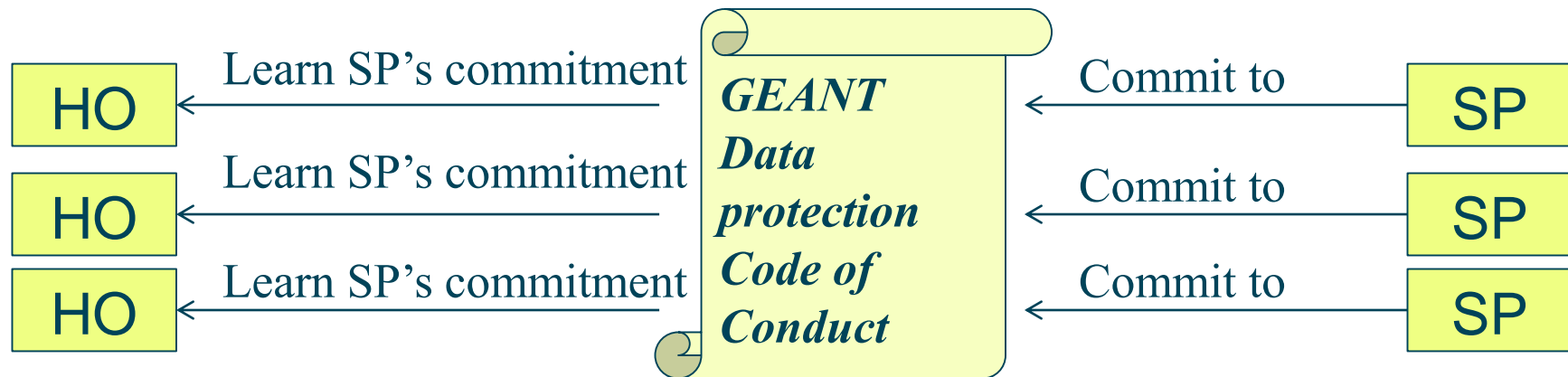
REFEDS Data Protection Code of Conduct (REFEDS CoCo)

VC 17 Feb 2014

Valter Nordh and Mikael Linden

- GÉANT Data protection Code of Conduct: for attribute release **between EU/EEA countries** and those with adequate data protection
 - EU28 + Norway, Iceland, Liechtenstein
 - Switzerland, Argentina, some sectors in Canada, US safe harbour...
 - Approved 14 June 2013
 - Available: https://refeds.terena.org/index.php/Data_protection_coc
 - Adoption started in Europe
- REFEDS Data Protection Code of Conduct: for attribute release from a Home Organisation in EU/EEA **to an SP outside EU/EEA**
 - Initial draft 29 July 2013 by DLA Piper
 - https://refeds.terena.org/index.php/International_dp_coc
 - Community consultation 12/2013

GÉANT Data Protection Code of Conduct for attribute release in EU



For more information on the GÉANT DP Code of Conduct:

- https://refeds.terena.org/index.php/Data_protection_coc
- TNC speak: <https://tnc2013.terena.org/core/presentation/8>
- TNC fullpaper: <http://tnc2013.terena.org/getfile/871>

The European approach to release of personal data out of EU/EEA



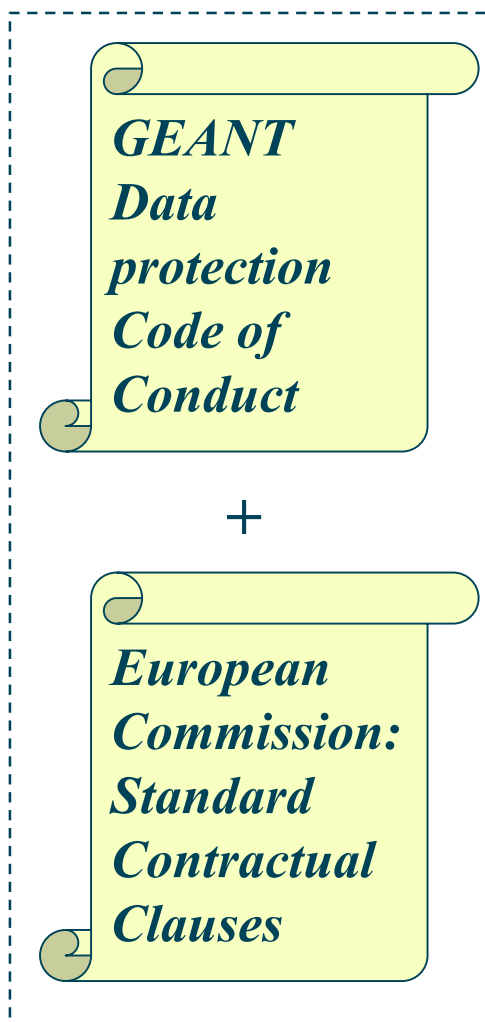
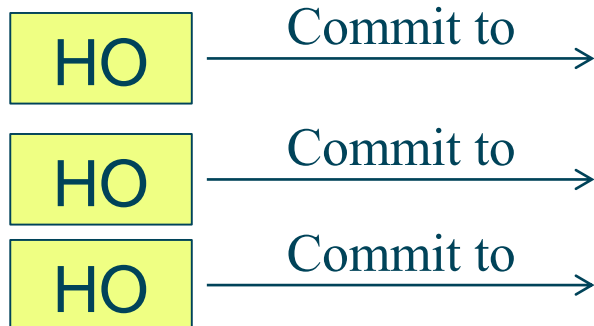
- Adequate protection of personal data must be guaranteed
 - Either by law (e.g. in EU, Switzerland, Argentina...)
 - Or by data importer voluntarily committing to EU-level protection
- Standard Contractual Clauses: EC-approved model contracts for data exporters (Home Organisations) and data importers (Service Providers) to sign
 - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF>
 - Basis for our REFEDS CoCo approach

REFEDS Code of Conduct

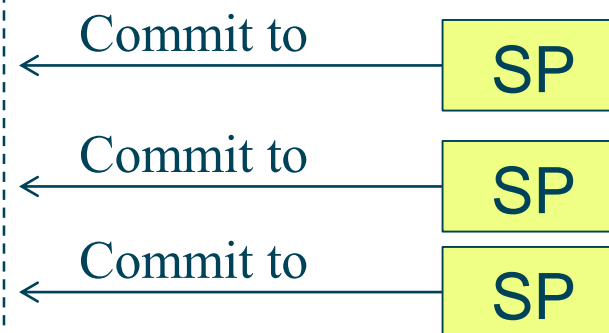
For attribute release out of EU/EEA



In EU/EEA



Outside EU/EEA



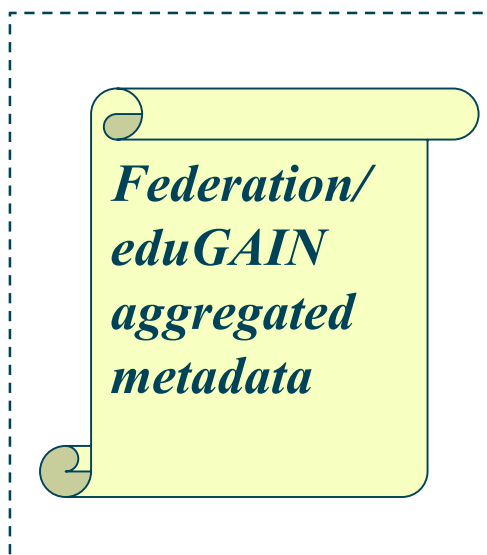
Technical representation on SAML2 metadata



In EU/EEA

HO

SAML2.0
metadata



Outside EU/EEA

SAML2.0
metadata



SP

- Entity category (support?) attribute:
"I'm committed to REFEDS CoCo"

- Entity category attribute:
"I'm committed to REFEDS CoCo"
- Md:RequestedAttribute
- Mdui:PrivacyStatementURL
- Mdui:DisplayName
- Mdui:Description

- Do we need a jurisdiction metadata tag for SPs?
- Co-existence of SP's Entity Categories?
 - E.g. SP supports both REFEDS CoCo and R&S
 - R&S specifies an attribute bundle, REFEDS CoCo not
- Interference of IdPs' Entity Category support attributes?
 - E.g. IdP has both REFEDS CoCo and R&S EC support attributes

Backup slides

Normative documents:

- Data Protection Code of Conduct for SPs in EU/EEA
- SAML2 profile for the DP CoC
- Entity category attribute definition for the DP CoC

Non-normative, informational documents:

- Introduction
- Introduction to the DP directive
- Risk management
- Privacy policy guidelines
- What attributes SP can request
- Good practice for Home Organisations
- Federation operator guidelines
- Handling non-compliance
- IdP GUI guidelines

https://refeds.terena.org/index.php/Data_protection_coc

GÉANT Code of Conduct: Service Providers commits to



Directly from the DP law

- Data minimisation
- Data retention
- Information security
- Informing the end user
- Data release out of EU/EEA

Further specifies the DP law

- Legal grounds: "attributes that are necessary..."
- Purpose: "enabling access"
 - Deviating purpose: on user consent only
- Release to 3rd party: on user consent or 3rd party committed to CoC
- Report security breaches

Read the full Code of Conduct text in:

https://refeds.terena.org/index.php/Code_of_Conduct_for_Service_Providers

SAML 2.0 metadata profile supporting the Code of Conduct



Standard SAML 2.0 metadata elements used to convey SP's relevant properties to a Home Organisation:

- Indication of SP's commitment to the CoC (Entity Category element)
- List of attributes the SP needs (`md:requestedAttributes`)
- Link to the SP's Privacy policy document (`mdui:privacyStatementURL`)
- SP's name (`mdui:displayName`)
- SP's description (`mdui:Description`)

Informing the end user on release of his/her personal data



Service name Weblicht

Description WebLicht is a service for language research. It provides an execution environment for automatic annotation of text corpora.

[Privacy policy](#)

Your following information will be released

Unique ID	mlinden@csc.fi
Name	Mikael Linden

OK