~~eduGAIN~~ GEANT Data Protection Code of Conduct (DP CoC)

Update

20.5.2012 REFEDS in Reykjavik

Mikael.Linden@csc.fi

Goal of the DP CoC

- **Ease the release of attributes** from Home Organisations (HO) to Service Providers (SP)

  => Make it easier for end users to log into SPs (in different federations/countries/jurisdictions)
- Try to make it in a way which is **sufficiently compliant** with the EU data protection directive
  - Balance the risk of non-compliance with value of easy collaboration
  - Sharing related responsibilities between the HO and SP
  - Remain scalable when the # of HOs and SPs grows
- Try to reduce Home Organisations' **hesitation to release attributes**
  - Seek for ways to avoid HOs becoming liable for SP's misbehaviour
  - Cf. "Research Collaboration needs" presented by David Kelsey

The short history

- 4/2011 eduGAIN policy was approved
  - Including eduGAIN Data Protection Good Practice Profile
- 5/2011 REFEDS attribute release wg and eduGAIN joins forces
- 6/2011 eduGAIN receives legal guidance from a lawyer (DLA Piper)
  - ”Data Protection Good Practice Profile is legally too weak”
- 12/2011 first draft of a minimal SP Code of Conduct
- 2/2012 Code of Conduct workshop in Brussels
  - Received positive feedback and proposed refinements
- 3/2012 1st call for comments
- Start to discuss with WP29 (EU data protection working party)

- 5/2012 2nd draft of SP Code of Conduct
- 6/2012 2nd call for comments on SP Code of Conduct

EU Data protection directive and federations

Innovation through participation

EU Data protection directive Definitions

- **Personal data**: ” any information relating to an identified or identifiable natural person”
  - Lawyer: assume any attribute (ePTID and even eduPersonAffiliation) counts as personal data
- **Processing of personal data**: ”any operation or set of operations on personal data, such as collection, …, dissemination,… etc”
  - Both IdP and SP processes personal data
- **Data Controller**: organisation which alone or jointly with others determines the purposes and means of the processing of personal data
  - IdP and SP (usually) are data controllers
  - Federation (and interfederation) may be joint data controller

EU Data protection directive
Obligations to data controllers (1/3)

Security of processing

- The controller must protect personal data properly
- Level of security depends e.g. on the sensitivity of attributes

=> *Federation policies, use of TLS and endpoint authentication, federation operator's practices…*

Purpose of processing

- Must be defined beforehand
- You must stick to that purpose

=> *Purpose of processing in IdPs: ~to support research and education*

=> *SPs' purpose of processing must not conflict with this*

EU Data protection directive
Obligations to data controllers (2/3)

Relevance of personal data

- Personal data processed must be adequate, relevant and not excessive
- *SPs must request and IdPs must release only relevant attributes*
- *=> md:RequestedAttribute*

Controller must inform the end user

- when attributes are released for the first time
- *SP's name and identity (=>mdui:Displayname, mdui:Logo)*
- *SP's purpose (=>mdui:Description)*
- *Categories of attributes processed (=> uApprove or similar)*
- *Any other information (mdui:PrivacyStatementURL)*
- Layered notice!

EU Data protection directive
Making data processing legitimate

a. User consents, or
b. Processing is necessary for performance of a contract to which the user is a subject, or
c. The controller has a legal obligation to process personal data, or
d. Necessary for vital interests of the user, or
e. Necessary for a task carried out in public interest, or
f. Necessary for the legitimate interests of the data controller

- Lawyer: Use (f): the SP has legitimate interests to provide service to the user
  - When the user expresses his willingness to use the service (e.g. by clicking ”log in” link)

Summary: EU data protection directive in very short

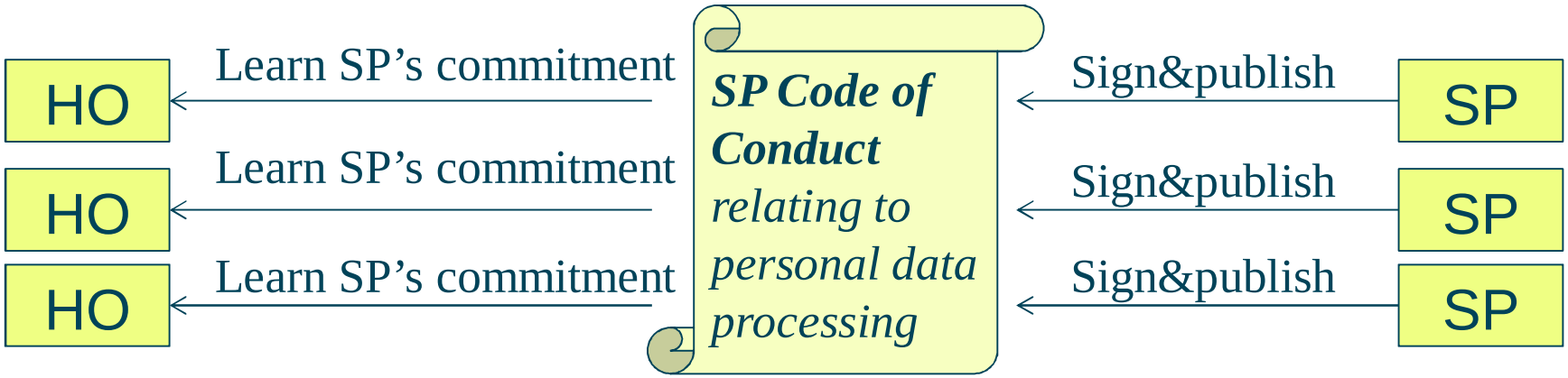
- Process personal data **securely**
- Use personal data only for a pre-defined **purpose**
- **Inform** the user
- Data **minimisation** (Minimal disclosure)
- Service Provider's **legitimate interests** as the legal grounds
- If attributes released **out of EU/EEA**, some more paperwork needed

- We seem to be coverging on these interpretations
- The proposed General Data Protection Regulation does not change the big picture, but there are some updates

GEANT Data Protection Code of Conduct approach

Innovation through participation

Data Protection Code of Conduct approach



- Voluntary to SPs (but SPs have interest to sign to receive attributes)
- Voluntary to Home Orgs to rely on (but may ease IdP admin's work)
- Nothing binds to GEANT/eduGAIN only
  - could be used internally in a federation, too
- It's not so difficult!

The SP Code of Conduct details

Second call for comments

- Target of the call for comments
  - Home Organisations (represented by and the comments gathered by the federation operators)
  - Service Providers (e.g. international research collaborations)
- Starts in the beginning of June
  - Follow refeds@terena.org mailing list
- Service Provider Code of Conduct
  - Plus a short introduction
  - Plus a template for comments

- Deadline for comments: 1st of Aug, 2012
- Comments and the resolutions by REFEDS attribute release wg and eduGAIN project will be published

Technical implementation

- SPs MUST populate in their metadata
  - Mdui:DisplayName, mdui: Description, mdui:PrivacyStatementURL
  - (Mdui:Logo is MAY)
  - Md:RequestedAttributes (with isRequired=”true”)
  - New <mddp:SPCoC> element
    - *a link to a signed copy of the Code of Conduct for SPs*
    - *Version identifier of the document that is signed*
    - *SP’s jurisdiction*
- SP’s Home Federation makes some sanity checks
  - Links resolve to proper existing documents etc
- Federations just mediate SPs’ metadata to the IdPs
- IdPs SHOULD present a GUI to inform the user of the attribute release
  - c.f. The uApprove update by Gakunin

Documentation supporting the Data protection Code of Conduct

- General documents
  - Introduction to Data protection directive
  - Managing data protection risks
- GEANT Data protection Code of Conduct
  - Service Provider Code of Conduct (”**the Document**”)
  - **Privacy Policy** guidelines for Service Providers
  - What **attributes** are relevant for Service Providers
  - Data protection **good practice for Home Organisations**
  - Federation **operator’s** guidelines
  - Handling **non-compliance**
  - **SAML2 profile** for the Code of Conduct
  - Notes on implementation on the **inform/consent UI**
- https://refeds.terena.org/index.php/Data_protection_coc
- **Do you want to have a separate call for comments on these?**

Next steps

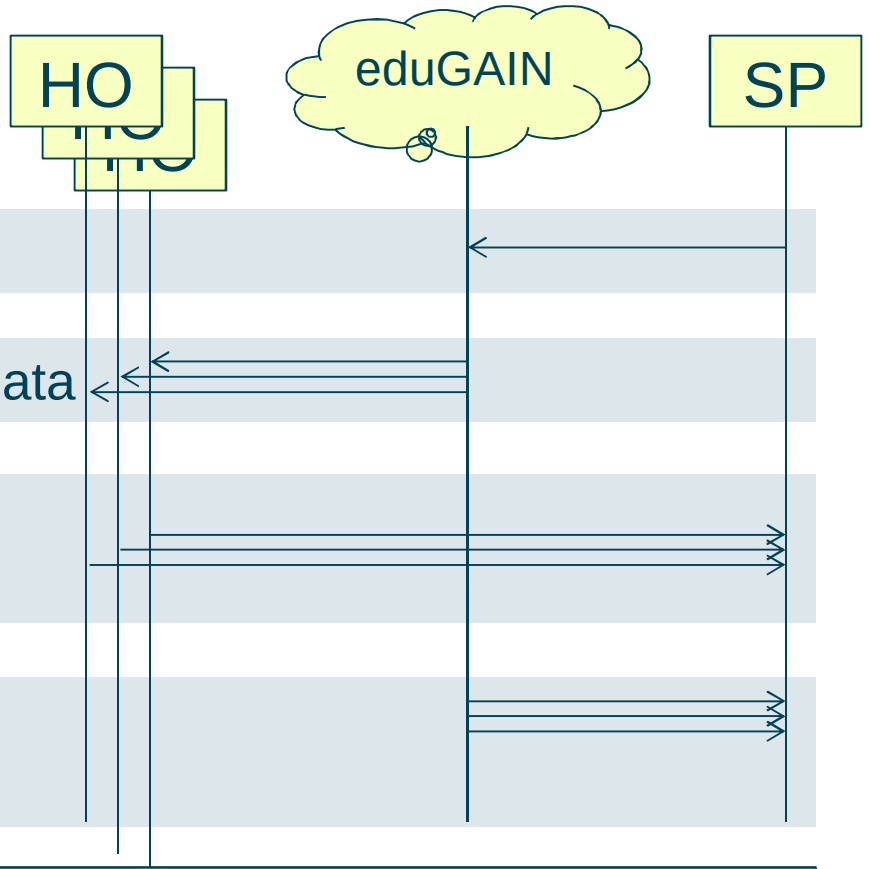
- Adoption
  - Pilots in autumn. Any volunteers?
- Expansion to non-EU/EEA countries
  - Requires developing additional documentation, based on EU model contracts, signed by HOs and SPs
- Phase 2: release of optional extra attributes on user consent

End of Data Protection Code of Conduct speak.

About federation harmonisation

Process for an SP joining eduGAIN

HO=Home Organisation



1. SP opts-in to get exposed to eduGAIN
2. HOs decide if they consume SP's metadata
3. HOs decide what attributes to release (DP Code of Conduct may help here)
4. SP decides which HO's metadata to consume

This is too complicated!
Service Provider communities will find an easier way!
e.g. Social network identity or issue local uid/pwd

The current model won't fly in a large scale

- Why do we have this complexity??
  - Because the federations have inequal policies!
  - Each Provider is bound by its local federation policy

  => Opt-in principle – A Provider acknowledges it understanding that the peer Provider is playing with different rules
- How to overcome this?
  - Need to harmonise our federation policies
  - To the extend that a Provider knows all peer Providers are playing with (sufficiently) similar rules