SUNET

Code of Conduct

för

tjänsteleverantörer (SP)

Code of Conduct (eduGAIN)

- Inom interfederationen eduGAIN finns ett förslag på en modell ***Code of Conduct*** (CoC) där SP ensidigt kan deklarera att de hanterar personuppgifter korrekt och att de endast begär nödvändiga attribut för att tjänsten ska fungera, den s.k. minimalitetsprincipen
- CoC gäller endast personuppgifter med liten risk
- CoC innebär att det är möjligt för en IdP att fatta automatiska och informerade beslut om överföring av personuppgifter till en SP
- CoC kommer att genomföras i begränsad pilot för ett fåtal tjänster i några få länder i Europa under hösten 2012

Attributöverföring från IdP till SP

Attribut som skickas delas in i två olika kategorier:

- Direkt personinformation
  - Exempel: namn, e-postadress, personnummer, pseudonym identifierare, eduPersonPrincipalName
- Indirekt personinformation
  - Organisationsinformation
    - Exempel: organisationsnamn, organisationsland
  - Övrig information t.ex. auktorisering
    - Exempel: eduPersonAffiliation, eduPersonEntitlement
  - Teknisk information (IdP, IP-adress mm.)

Överföring av personinformation

- Personinformation i attributöverföring är behandling av personuppgifter
- För behandling av personuppgifter gäller PUL (om inte annan lag gäller)
  - Exempel på annan lag som gäller utöver PUL är Förordning (1993:1153) om redovisning av studier m.m. vid universitet och högskolor

Överföring av personuppgifter

- PUL säger att personuppgifter får behandlas utan samtycke om behandlingen är nödvändig
- Detta innebär att en IdP endast får skicka nödvändiga attribut för att tjänsten ska fungera utan att användaren behöver ge sitt aktiva samtycke, den s.k. minimalitetsprincipen i Code of Conduct

Överföring av personnummer

Personuppgiftslagen 22 §

- Uppgifter om personnummer eller samordnings-nummer får utan samtycke behandlas bara när det är klart motiverat med hänsyn till
  a) ändamålet med behandlingen,
  b) vikten av en säker identifiering, eller
  c) något annat beaktansvärt skäl.
- Personummer kan aldrig överföras med hjälp av Code of Conduct beroende på PUL 22 §

Överföring av personuppgifter till tredje land

Personuppgiftslagen 33 §

Det är förbjudet att till tredje land föra över personuppgifter som är under behandling om landet inte har en adekvat nivå för skyddet av personuppgifterna. Förbudet gäller också överföring av personuppgifter för behandling i tredje land.

- Enligt 34 § är det tillåtet att överföra personuppgifter efter samtycke till överföringen eller om överföringen är nödvändig (t.ex. fullföljande eller tecknande av avtal)
- Enligt 35 § är det i vissa fall även tillåtet med överföring om tillräckligt skydd finns, s.k. safe harbor