Science & Technology Facilities Council

EU AAI Legal Issues

David Kelsey (STFC-RAL)

DESY

22 Jan 2014

Overview

- Data Protection in the EU
- AAI and data protection
- eduGAIN and REFEDS developments
- New EU data protection regulation
- Some views from Andrew Cormack – janet(uk)
- Conclusions

Data Protection

- EU Directive 95/46/EC
  - On the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Personal Data
  - any information relating to an identified or identifiable natural person

Data processing only allowed if one of these:

- when the data subject has given his consent
- when the processing is necessary for the performance of .. a contract
- when processing is necessary for compliance with a legal obligation
- when processing is necessary in order to protect the vital interests of the data subject
- for the performance of a task carried out in the public interest, …
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, …

In Research and Education AAI – often felt that consent would work

- BUT, this only works if consent is freely given (not for doing a job)
- Now concentrating on "legitimate interests"

Data Protection and AAI

- Early use cases of federations revolved around role-based attributes (student, faculty member, …)
  - E.g. access to e-Journal where name and identity is not needed
- eduPersonTargetedID
  - Unique, persistent, opaque handle per person per SP
- Some places where this may even be considered personal data
- IP addresses are sometimes personal data too!
- For AAI for Research
  - AuthZ often needs identity and to be able to contact person
  - E.g. Access to medical data granted by ethics committee
  - EGI VOs require access to User-level job accounting data
    - IGTF certificates contain a real CommonName and often an email address
    - Need Formal Policy to control this accounting data

eduGAIN and REFEDS developments

- SP Code of Conduct
  - Goal is to increase trust between Home Organisations and Service Providers and thus facilitate attribute release
- Research & Scholarship Entity Category

CoC: Recommended IdP attributes

- displayName
- cn
- mail
- eduPersonAffiliation, eduPersonScopedAffiliation,
- eduPersonPrincipalName,
- SAML2 Persistent NameID (eduPersonTargetedID),
- schacHomeOrganization
- schacHomeOrganizationType

REFEDS R&S Category

- Service Providers that support research and scholarship interaction, collaboration or management as an essential component
- Service Providers SHOULD request a subset of R&S Category Attributes that represent only those attributes that the Service Provider requires to operate its service
- Identity Providers are strongly encouraged to release the following bundle of attributes to R&S category Service Providers:
  - personal identifiers: email address, person name, eduPersonPrincipalName
  - pseudonymous identifier: eduPersonTargetedID
  - affiliation: eduPersonScopedAffiliation

New EU data protection regulation

- Draft made in 2012, but still a long way from implementation
- Key changes
  - Right to be forgotten
  - Explicit consent rather than assumed (where required)
  - Companies will need to notify data breaches within 24 hours
  - A single set of rules for all EU countries
  - Companies deal with a single national data protection authority
    - In the country in which they are mainly established
  - Individual right to refer all cases to their home authority
  - EU rules will apply to all external companies if they offer services or monitor EU citizens
  - Strengthened national authorities and increased penalties

Legal recommendations in the EC AAA Study

For consideration in the new DP regulations

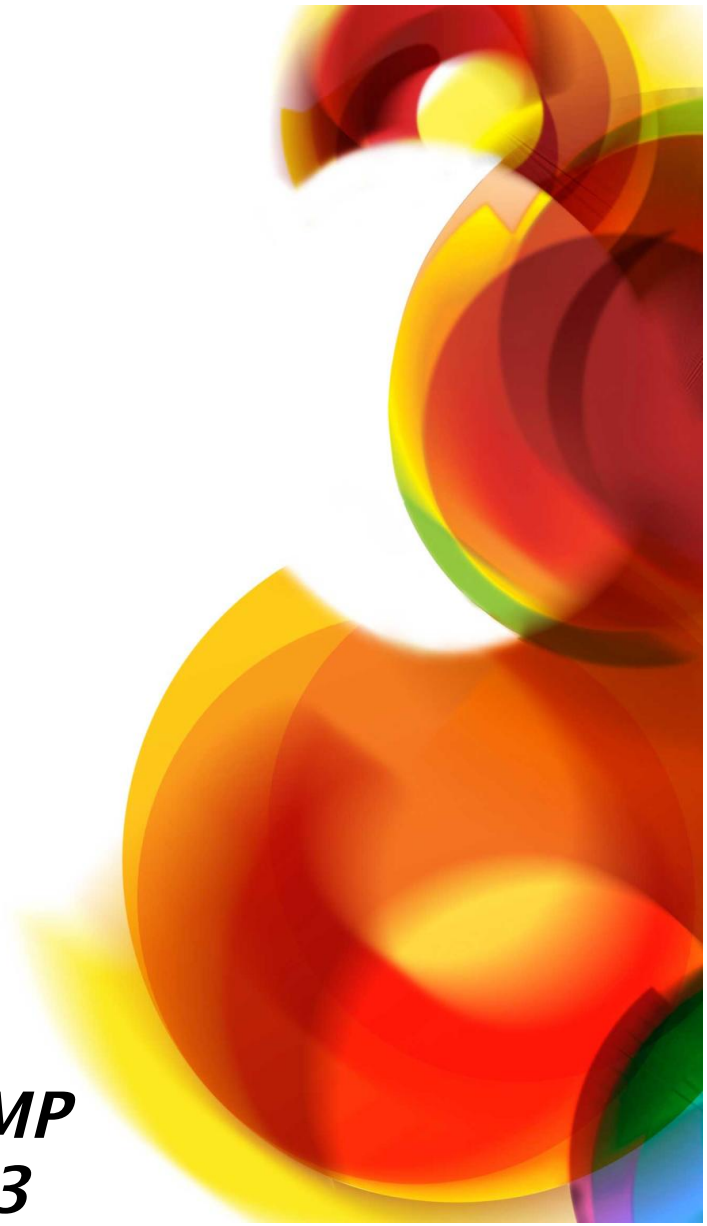
- Extend the Legitimate Interests justification to cover international transfers
- The EC should provide clarity about Consent and Legitimate Interests
- EC should study how adequate protection can be achieved in lightweight agreements between researchers and others
- EC and Article 29 WP should give clear statement on processing opaque identifiers
- EC should train member states to avoid differences
- Member states laws should be aligned with EC laws

janet

VAMP Year 2: Day 1

Andrew Cormack
Chief Regulatory Adviser, Janet
@Janet_LegReg

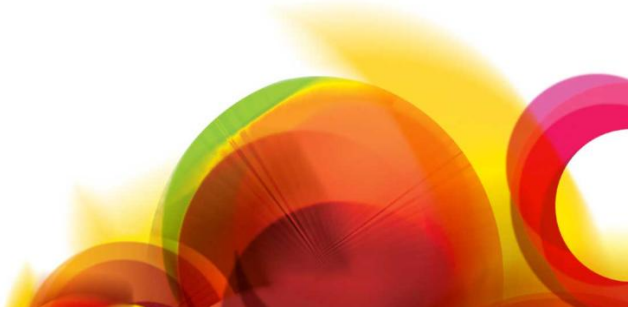
Shown in Helsinki VAMP meeting 30 Sep 2013



It's the politics, stupid

janet

- Draft Data Protection Regulation now deep in politics
  - Basic disagreement on what individuals want
  - Parliament & Council haven't reached **initial** negotiating positions
  - >3000 amendments proposed
  - Privacy experts want to start again!
- And then PRISM
  - "No Personal Data release to countries that spy"
  - Errr... Plenty of those **inside** the EU!
- Federation needs unlikely to be heard in the noise ☹



janet

Where now?

US public domain by Fish & Wildlife Service/Wikimedia Commons

Back to basics

janet

- Minimise data/processing
  - Whatever privacy law emerges, less is going to be better
- Minimise surprise
  - Happy users won't complain to lawyers
- Reduce (regulatory) risk, don't hope to eliminate it
  - Aim: benefit outweighs risk

Minimisation

Benefits of single identity may justify ePTID pain (Jens)

Services need (just) adequate and relevant data (Jens)

Zero-attribute authN (Remco)/Last-resort IdP (Marco)

- Find out what SPs **really** need

Identify user only for accounting/audit (Marco)

- Maybe it's enough to know those policies/processes exist?

Negotiate access vs attribute provision (Jens)

Support VO-specific attributes (e.g. %FTE) (Heather)

Surprise

janet

Use “account” as a way for user to view/control data flow (Jens)
Allow users some control of policies (Jens)
Let communities define own location/access policies (Johannes)
‘Goldilocks’ complexity (Heather)

Silently “just working” => hard to excite users (Frank)

Risk/Benefit

janet

Willingly accept the risk of reliance on a person/entity/system to act [in way that helps] (Bob Cowles)

Entity categories as risk/benefit categories (pers.comm.)

Without clear law, this seems the only approach...

Conclusions

- Minimise use of personal data
  - Restrict the required list of attributes from IdP
- Codes of Conduct and Categories seem a good way forward
  - Scalable negotiation
- Will the data protection authorities agree?

Questions?