

# EGI (WLCG) Data Protection

David Kelsey - UKRI  
EUGridPMA meeting 23 May 2022  
LRZ, Garching

# History

- Existing EGI policy on Data Protection (2015 to 2017) - with AARC and WLCG

<https://documents.egi.eu/document/2732>

- Based on EU Directive 95/46/EC (not GDPR)
- Lots of consultation with GEANT, REFEDS, R&E federation lawyers
- AARC deliverable addressed this in deliverable DNA3.5
- Personal Data collected as a result of Grid Operations
  - Not sensitive - just R&S attributes
- All sites are Data Controllers
- Bi-lateral contracts not possible - too many sites and no central controller
- Risks to end users are very small
- User Consent does not work
- Legal Basis - Legitimate Interest
- “Lightweight” Binding Corporate Rules (BCR)-like approach
  - But no monitoring and limited control of legal/financial responsibility

# AARC Guidance

Deliverable DNA3.5: Recommendations and Template Policies for the Processing of Personal Data.

[https://aarc-project.eu/wp-content/uploads/2018/03/AARC-DNA3.5\\_Recommendations-for-Processing-Personal-Data\\_2016\\_11\\_07\\_v4\\_DG.pdf](https://aarc-project.eu/wp-content/uploads/2018/03/AARC-DNA3.5_Recommendations-for-Processing-Personal-Data_2016_11_07_v4_DG.pdf)

Data Protection Impact Assessment - an initial guide for communities

<https://aarc-project.eu/wp-content/uploads/2018/05/AARC-G042-Data-Protection-Impact-Assessment-initial-guidance-for-communities.pdf>

Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

<https://aarc-project.eu/wp-content/uploads/2018/03/AARC-G040-Preliminary-Policy-Recommendations-for-the-LSAAI-RandS-and-DPCoCo.pdf>

# GDPR era (2018 onwards)

- Code of Conduct now a supported part of regulation
- GEANT working on new (V2) DPCoCo - this could help lots with international transfers of operational data (accounting etc)
- Decided to concentrate on producing a Privacy Notice
  - Did this for WLCG
    - <https://wlcg-docs.web.cern.ch/?dir=policy/security>
  - EGI Foundation was taking care of its own
    - And was exploring possibility of Controller-Processor DP agreements everywhere
    - This approach was not followed (except for sub-contracted core services)
- Waiting for GEANT CoCo V2
  - This has now been published – but not a Code of Conduct
  - Guidance for best practice
  - <https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home>

# Data Protection Policy (WLCG) - work in 2019

- Agreed a Privacy Notice for WLCG (July 2019)
  - And use of WISE Baseline AUP v1
- Produced an updated version of the 2017 DP Policy
- Only a few changes needed for GDPR era
  - In section 5 vii - Requirement for a PN)
    - No longer require a named DPO
    - PN must specify the legal basis for processing
- Then lots of WLCG discussion
  - Data retention - maximum 18 months
  - To where does User report issues?
  - To where do we report breaches?
  - And lots of concern about the wording (this had not been questioned back in 2015-17)

# Next steps

- Work on updating AARC GDPR guidance
- Regular meetings of the WISE SCI-WG
- EOSC Future DPMS (See David Groep talk)
- Draft google doc
  - [https://docs.google.com/document/d/11S5UrCytHdeh4mNQc3btvZPW\\_ox\\_QgSBx0III-XhKol/edit?usp=sharing](https://docs.google.com/document/d/11S5UrCytHdeh4mNQc3btvZPW_ox_QgSBx0III-XhKol/edit?usp=sharing)
- We can (at this meeting) discuss and make progress on this draft