Science & Technology Facilities Council

PERSONAL DATA PROCESSING

INTRODUCTION TO PROPOSED NEW DRAFT POLICY ON THE PROCESSING OF PERSONAL DATA

IAN NEILSON – STFC RAL

13 January 2016

Personal Data Processing

- Background context
- Possible approaches
- Outline of draft proposal
- Considerations

Disclaimer

I AM NOT A LAWYER

Background context - 1

- Ongoing review and update of currently endorsed policies
- Increased sensitivity and awareness of privacy issues
- Several policies deal directly or indirectly with “Personal Data”
    - User Level Job Accounting
    - VO Registration: *email and DN ….*
    - Traceability and Logging:
      “ … identify the source of all actions … and the individual who initiated them”
    - *…*

Background context - 2

- Provide a common policy on storage and transfer of Personal Data
  - Backed up by separate implementation guidance docs.
- International transfers
  - Clarify and enable transfers across WLCG and EGI *including* outside of EU or EEA
- Position updated policy in anticipation of updated EU regulations
  - Press release 15 Dec 2015:
    - *"Agreement on Commission's EU data protection reform…"*
  - *"Data Protection Authorities will work more closely together …"*
  - Target date 2018

Possible approaches - 1

- Shaped by rules on International transfers
  - Countries “without adequate safeguards”
  - EU participants of course have “common” framework anyway
- Options:
  - User Consent
  - ~~Safe Harbor~~
  - Model Contracts
  - Adequate safeguards
  - Binding Corporate Rules

Possible approaches - 2

- User Consent
  - *"..must be freely given, specific, informed and unambiguous indication of data subject's wishes.."*
  - strictly interpreted on a per transfer or transfer class basis
  - are researchers "free" if to say no prohibits their work?
- ~~Safe Harbor~~
  - self assertion to rules.
  - only applicable to US entities but not research labs anyway
  - now killed by EU court ruling October 2015

Possible approaches - 3

- Model Contracts
  - bi-party *controller-to-controller*
  - fixed, unalterable clauses from the EU
  - proposed for use in GEANT International DP Code of Conduct
  - hard to frame outside of one-way (attribute release) use case
  - would require a mesh of agreements
- Adequate Safeguards
  - controllers make own adequacy assessments
  - risks of inadequate assessment
  - very little used and not permitted by some EU States
  - again, one-way 'point-to-point'

Possible approaches - 4

- Binding Corporate Rules (BCR)
  - codes of conduct adopted within an international organisation
  - UK DPA quotes –
    - *"..designed to be a global solution for multinational companies by ensuring their intra-group transfers comply with the eighth principle…"*
    - *"The main advantage of BCRs over other means of providing adequate safeguards is that, once developed and operational, BCRs can provide a framework for a variety of intra-group transfers to meet your organisation's requirements."*
  - Article 29 Working Party provided guidance table for formulation
  - Still not a panacea
    - *".. obligation to monitor your compliance .. include regular audits .. training programme for staff handling personal data."*
    - and see Considerations below ….

Outline of draft proposal - 1

- Infrastructure is bound by a single policy set
  - Assume BCR can be appropriate

- Take the Directive and BCR guidance and ..
- .. with regard to the risk exposed ..
- .. handle as many of the requirements as possible.

- Keep it clear and simple

- Current Draft here: https://documents.egi.eu/document/2732

Outline of draft proposal - 2

- Policy Structure
  - INTRODUCTION
  - DEFINITIONS : Infrastructure; Participant; Personal Data; Processing; End User
  - SCOPE : What is covered, and what is not
    - one policy applies to all types of Personal Data storage and transfer but …
    - excluding Personal Data in research datasets
  - POLICY : Agreement to Principles and sanctions on failure (exclusion)
  - PRINCIPLES OF PERSONAL DATA PROCESSING : 8 clauses
  - REFERENCES
  - INFRASTRUCTURE PARTICIPANT EXAMPLE PRIVACY POLICY
    - making it as easy as possible to prepare per use-case policies

Outline of draft proposal - 3

- PRINCIPLES OF PERSONAL DATA PROCESSING
  i. Fair and lawful
  ii. Purposes
    - Administrative, operational, accounting, monitoring and security
  iii. Adequacy
  iv. Accuracy
    - Correcting errors
  v. Retention
    - Period defined in relevant policy or default 18 months
  vi. Technical and organisational security
    - Measures for protected storage and transmission
    - Participant Data Protection Officer with contact points etc.
    - Audits and Incident Response

Outline of draft proposal - 4

- PRINCIPLES OF PERSONAL DATA PROCESSING cont.

vii. Rights

- Privacy Policy clearly presented to End User
- Include who, what, why and for how long plus ..
- .. rights and procedures for query (i.e. via DPO)
- Example Privacy Policy provided as template

viii. Transfer restrictions

- Only within Infrastructure bound by common policies
- Covers International Transfers
- Clause to allow for incident response

Infrastructure Participant Example Privacy Policy

This Privacy Policy explains how we, *[insert Participant name here]* ("We"), treat data by which you can be personally identified ("Personal Data") as a result of your registration for and use of *[insert Infrastructure name here]* ("Infrastructure").

We collect the following Personal Data to identify you to enable us to grant you access to the Infrastructure and the services such as compute, storage and network that its participants offer:

- Name
- Email address
- Affiliation (e.g.VO)
- Certificate Distinguished Name (DN)
- *[Add or remove data as appropriate]*

To enable the Infrastructure to be safe and reliable for your use and to preserve your rights as a user we adhere to The Policy on the Processing of Personal Data ("The Policy") available here: *[insert url to PPPD here]*.

Your Personal Data will be shared but only where -

1. The recipient has agreed to abide by The Policy or
2. Doing so is likely to assist in the investigation of suspected misuse of Infrastructure resources.

Your usage of the Infrastructure will be monitored. Records of this use, containing your Personal Data, may be shared as described above for operational, security and accounting purposes only. These records will be purged or anonymised after, at latest, 18 months.

You can contact our **Data Protection Officer** (*[insert contact details here]*) to obtain a copy of your Personal Data, request that it is corrected in case of factual error or if you suspect that it has been misused. You can also request that we stop using your Personal Data but this will affect your access to the Infrastructure.

This Policy should be read with reference to the Policy on the Processing of Personal Data and other Infrastructure policies available at *[insert link to Infrastructure Policies here]*.

[Insert Name and Contact Details of Participant]

Considerations

- We are clearly not a corporate body
- BCRs are "*subject to authorization by relevant DP authority*"
- Impossible to legally assign risks and liabilities

BUT

- Risks of harm to the End User and liabilities are very small.
- We use an approach which follows the principles and spirit of the Directive being open and accessible to End User and Participant.
- May be the best that is possible without a heavyweight, disruptive (and expensive) approach.

Considerations

It may also be worth considering whether BCRs could be used for transfers within a community cloud. Although community members are not necessarily part of the same corporate group, they may have enough interests in common, such as government authorities or highly regulated sectors such as financial services or pharmaceutical companies, that it may be feasible for them to agree and sign up to a single legally binding self-regulatory code which will be enforceable by data subjects.

- Cloud Computing Law – Millard et al. 2013 (p 273)

Thank You

Acknowledgement to Dave Kelsey, Hannah Short, Romain Wartel and others.

Science & Technology
Facilities Council