WLCG & GDPR

David Kelsey (STFC UK Research and Innovation)
WLCG GDB – 12 Sep 2018

eosc-hub.eu

@EOSC_eu

EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 777536.

HISTORY – In April 2018, I proposed

- **WLCG and Experiment services should abide by** (the to be submitted, unapproved) GÉANT Data Protection Code of Conduct V2
- For all services which consume/process personal information directly from end-users (e.g. workload management portals, user registries, data transfer portals, GOCDB, accounting, etc etc)
  - **Prepare and make easily available** an updated Data Privacy statement
  - Template will be provided (based on GÉANT Data Protection Code of Conduct)
- WLCG (Operations) should **create a register** of all such services
  - Together with contact names and copies of Data Privacy statements

WLCG MB 19 June 2018 – a plan of action

- At REFEDS meeting (10 June 2018)
  - The GEANT Code of Conduct V2 is still not finalized
  - Seems to be some way off (several contentious items)
- I am hearing growing number of concerns as to how long approval will take
- Discussions at TNC17 with David Foster and Andrew Cormack (how best to proceed?)
  - Produce a light-weight “Code of Conduct”-like framework for WLCG (and EGI/EOSC-hub)
    - To replace the existing EGI/WLCG Data Protection Policy Framework (not a Code of Conduct)
    - Write a general WLCG Data Privacy Statement and a template for others to use
  - All web portals and experiments also still need their specific one
- All WLCG sites bound to policy by the WLCG MoU (no need to sign anything new)
- The EOSC-hub/AARC2/WLCG policy team will prepare draft documents
  - Meeting at CERN (after July GDB) - discuss over summer
  - For presentation at September GDB and approval soon after
- WLCG Ops should continue building their list of services needing a Privacy Statement

News since July 2018

- The F2F policy workshop did happen at end of July
  - But we were fully occupied by work on AARC2 Policy Development Kit
    - And a new WISE baseline AUP (more on that topic in the coming weeks)
  - Little time left to work on GDPR
- Then holiday season!
- The replacement Data Protection Policy Framework will be worked on during the coming months
  - And next F2F policy meeting in early November 2018
- But we did make progress on
  - Risk assessment of need or otherwise for a Data Protection Impact Assessment
  - General WLCG Privacy Notice

Data Protection Impact Assessment (21 Aug 2018) Talk by Uros Stevanovic at WISE/NSF Cybersecurity Summit

AARC Authentication and Authorisation for Research and Collaboration

WISE Workshop

Data Protection Impact Assessment

Uros Stevanovic

KIT

NSF Summit 2018

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

Risk assessment and Data Protection Impact Assessment (DPIA)

GDPR Article 35(1) – "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing."

WP29-248 Opinion (Oct 2017)
When is DPIA necessary?

- One operation, or group of similar operations
- “Likely to result in high risks”, ten criteria
  - Evaluation or scoring
  - Automated decision making with legal or similar effects
  - Systematic monitoring
  - Sensitive data (or data of highly personal nature)
  - Data processing on a large scale
  - Matching or combining datasets
  - Data concerning vulnerable subjects
  - Innovative use or applying new technological or organizational solutions
  - Data transfer outside EU
  - Processing resulting in preventing data subjects from exercising a right or using a service or a contract
- Two or more → DPIA likely (but not necessarily mandatory)
- Sometimes even one is enough

CNIL guidance (France)

Severity

- Negligible:
  - Loss of time in repeating
  - Spam emails
  - Targeted advertising
  - Mere annoyance caused by information received or requested
  - Feeling of losing control of one's data
  - Feeling of invasion of privacy without real or objective harm (e.g. commercial
  - intrusion)
  - Loss of time in configuring one's data
- Limited:
  - Unanticipated payments, additional costs (e.g. bank charges)
  - Denial of access to administrative or commercial services
  - Lost opportunities of comfort (termination of an online account)
  - Minor but objective psychological ailments (defamation)
  - Feeling of invasion of privacy without irreversible damage
  - Intimidation on social networks
- The level of severity may be raised or lowered by including the following factors:
  - Level of identification of personal data
  - Nature of risk sources
  - Number of interconnections (especially with foreign sites)
  - Number of recipients (which facilitates the correlation between originally separated

French DP Authority (CNIL)

DPIA – risk table (CNIL)

Risks	Impacts on data subjects	Main risk sources	Main threats	Existing or planned measures	Severity	Likelihood
Illegitimate access to personal data						
Unwanted change of data						
Disappearance of data						

Privacy risks, security risks → can be considered together
Input from WISE risk management

WLCG Risk Assessment for DPIA

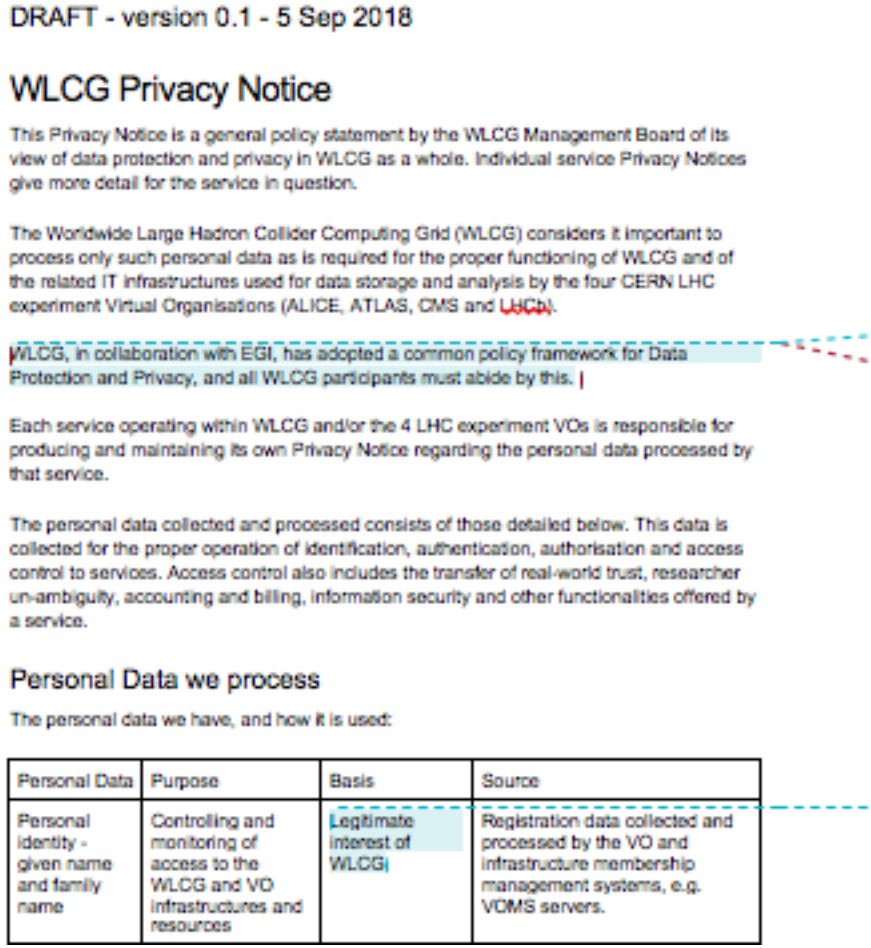
- We have drafted a risk assessment (but no meeting yet to discuss)
  - Given that we only process personal data like name & email address
    - ”Common personal data”
    - IP access logs are not sensitive
  - Risks to rights and freedoms of WLCG users are “negligible”
  - And likelihood is probably low
  - Therefore no need to perform a formal DPIA
- We will finalise this risk assessment and present to WLCG MB
- Need to do a regular review of this risk assessment

WLCG General Privacy Notice

- There are many existing templates, including one in CoCo version 2
- I proposed to use the new CERN template
  - https://odpp.web.cern.ch/sites/odpp.web.cern.ch/files/DPP-002-PrivacyNotices.pdf
- Contents of the template
  - Basis for processing of Personal Data by the Service
  - Processing Personal Data
  - Sharing data internally at CERN
  - Transfer data externally
  - Automated decision making and Profiling
  - Scale of service

WLCG Privacy Notice (2)

- This needs to be discussed and agreed by security policy team first
  - And we have to agree details like who should be quoted as “contact” points
  - Will do all this during September/October
- Will consult wider, including GDB, once ready



DRAFT - version 0.1 - 5 Sep 2018

WLCG Privacy Notice

This Privacy Notice is a general policy statement by the WLCG Management Board of its view of data protection and privacy in WLCG as a whole. Individual service Privacy Notices give more detail for the service in question.

The Worldwide Large Hadron Collider Computing Grid (WLCG) considers it important to process only such personal data as is required for the proper functioning of WLCG and of the related IT infrastructures used for data storage and analysis by the four CERN LHC experiment Virtual Organisations (ALICE, ATLAS, CMS and ~~LHCb~~).

WLCG, in collaboration with EGI, has adopted a common policy framework for Data Protection and Privacy, and all WLCG participants must abide by this.

Each service operating within WLCG and/or the 4 LHC experiment VOs is responsible for producing and maintaining its own Privacy Notice regarding the personal data processed by that service.

The personal data collected and processed consists of those detailed below. This data is collected for the proper operation of identification, authentication, authorisation and access control to services. Access control also includes the transfer of real-world trust, researcher un-ambiguity, accounting and billing, information security and other functionalities offered by a service.

Personal Data we process

The personal data we have, and how it is used:

Personal Data	Purpose	Basis	Source
Personal identity - given name and family name	Controlling and monitoring of access to the WLCG and VO infrastructures and resources	Legitimate interest of WLCG	Registration data collected and processed by the VO and infrastructure membership management systems, e.g. VOMS servers.

Message to WLCG sites/Experiments

- Most sites do not expose any service directly connected to by end users
  - Do not panic :=)
  - Can just use the general WLCG privacy notice (if even necessary)
  - Continue to abide by the existing Data Protection Policy Framework
    - And existing Policy on User-level Job Accounting
- Those who expose services directly to users will need their own Privacy Notice
  - LHC Experiments – User registration and group management (e.g. VOMS), Workload management portals, Data transfer/management portals, dashboards, monitoring etc.
    - If you need to show names on a dashboard must justify why in the Privacy Notice
  - Sites which expose services directly to users, e.g. VOMS, FTS portals, Dashboards, monitoring, accounting, GOCDB, etc.

Thank you for your attention

Questions?

Contact

David.Kelsey@STFC.ac.uk

EOSC-hub

eosc-hub.eu @EOSC_eu