WLCG & GDPR

David Kelsey (STFC-RAL)

WLCG Collaboration Workshop – Naples – 28 March 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.

EOSC-hub

WLCG & GDPR

(based on slides shown at Naples WLCG Workshop – 28 March 2018)

GDPR & WLCG?

Disclaimer – I am not a lawyer – these are SPG (non-expert) views.

And this is a very brief report on a complex topic!

- Many WLCG services consume personal data from X.509 certificates, IdPs and Community Attribute Authorities (Experiment Authorisation databases)
- We consider all such services (run by Sites or by VOs) in general are “Data Controllers”
- International Transfers (outside of EU) are essential for WLCG
  - In current EGI/WLCG Data Protection Framework we align ourselves with “Binding Corporate Rules” to control these transfers
- So what changes now under the GDPR?

Big thanks to Andrew Cormack (Jisc, UK) for slides he showed in webinars

GDPR – what is it?

- An EU Regulation (2016/679/EU) – applies to all member states
- Scope: all natural persons and all organisations/enterprises in Europe
  - And beyond, to orgs providing services to/collecting data from Europeans
- Not in scope: processing by a natural person in the course of a purely personal or household activity
- Replaces the old Data Protection Directive (1995/46/EC)
- Comes into force on 25th May 2018

GDPR – what is new? An incomplete list!

- Accountability (need to document)
  - » What, why, where, how long for, who may obtain it?
  - » Risks, and how they are managed
  - » Information lifecycles, not just asset registers
- Data Protection by Design/Default
  - Data minimisation, anonymisation, pseudonyms, etc.
  - Options default to privacy-protecting: users must choose to relax
  - Formal Data Protection Impact Assessments (DPIA) – risks to individuals
- Consent
  - New, tighter, conditions for consent to be valid
  - ***not*** a condition of service, ***not*** under compulsion
  - Designed to be hard to obtain/manage ("reduce overuse") – not relevant in most WLCG use cases!
- User Rights
  - Information, access, portability, rectification, erasure, objection, restriction, no automation
- Security
  - Must protect data, notify breaches and there is explicit support for security incident response

GÉANT Data Protection Code of Conduct V2

- Produced by GN4-2 (Mikael Linden, CSC, leading) with extensive legal advice
  - For all of Research and Education – including Research Infs and e-Infrastructures
- GDPR Articles 40 & 41 address “Codes of Conduct” (CoCo)
  - Associations and other bodies representing categories of controllers or processors may prepare codes of conduct
  - to provide appropriate safeguards within the framework of personal data transfers to third countries (*Service outside of EU abiding by CoCo V2*) the Controller inside EU must
    - make binding and enforceable commitments, via contractual or other legally binding instruments (*This is one area of discussion*)
  - Article 41 requires a body to monitor compliance with the CoCo
    - *What are the responsibilities and liabilities of this monitoring body?*
- CoCo V2 is limited to the processing of **Attributes which are released for enabling access to a Service**
  - Includes many related purposes (Authorisation, Accounting/Billing, Science gateways etc.)
- A new final draft being produced now for submission to Authorities at end of May 2018

Display names versus Pseudonymisation?

- GDPR encourages the pseudonymisation of personal data as a method of data protection
  - But an opaque persistent ID is still personal data (can be used to identify)
  - GDPR says “is not intended to preclude any other measures of data protection”
- The CoCo V2 recognises importance of:
  - **Researcher unambiguity** i.e. ensuring that a researcher’s scientific contribution is associated properly to them
    - notes that identifiers like ORCID are important
  - **a name attribute** (such as commonName or DisplayName attribute) is necessary for a wiki or other collaboration platform, if the End Users know each other in real life and need to be able to transfer their existing real-world trust to an online environment

What do WLCG participants need to do?

- **Abide by** (the to be submitted, unapproved) GÉANT Data Protection Code of Conduct V2
  - And of course the GDPR itself
- Comment (via WLCG GDB or join SPG) on modified Data Protection Policy Framework
  - EOSC-hub/AARC2 will produce draft for GDPR in coming weeks
- 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)
    - And updated EOSC-hub/WLCG framework
- WLCG (Operations?) should **create a register** of all such services
  - Together with contact names and copies of Data Privacy statements
- We (EGI SPG) need to write a risk statement (for end users) – one general one
  - Risks to rights and freedoms are very small (only names, institutes and email addresses)
  - French (CNIL) document on Privacy Impact Assessment – suggests our risks are “negligible”
- We should **prepare to make immediate** reports following any data breach

More information on GDPR issues

- With many thanks to Andrew Cormack, Jisc, UK – nice recorded webinars
- https://www.jisc.ac.uk/training/moving-toward-GDPR
- https://community.jisc.ac.uk/blogs/regulatory-developments/event/webinar-gdpr-practice
- GDPR Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
- GÉANT Draft Data Protection Code of Conduct V2 (29 Jan 2018): https://wiki.refeds.org/download/attachments/1606455/G%C3%89ANT%20Data%20Protection%20Code%20of%20Conduct%20v2_29Jan2018.pdf
- Mikael Linden (CSC, Finland) – webinar on the V2 Code of Conduct https://www.youtube.com/watch?v=xF1L57Cvumg

Thank you for your attention

Questions?

Contact

David.Kelsey@STFC.ac.uk

EOSC-hub

eosc-hub.eu @EOSC_eu