Implementing General Data Protection Regulation for Research Data

Digital Infrastructures for research
28-30 September 2016, Krakow

Urpo Kaila
EUDAT Security Officer
urpo.kaila@csc.fi
security@eudat.eu
A truly pan-European Infrastructure

EUDAT offers common data services, supporting multiple research communities as well as individuals, through a geographically distributed, resilient network of 35 European organisations.

The EUDAT vision is to enable European researchers and practitioners from any research discipline to preserve, find, access, and process data in a trusted environment, as part of a Collaborative Data Infrastructure.
B2 Service Suite

- **B2DROP**: Sync and Exchange Research Data
- **B2SHARE**: Store and Share Research Data
- **B2SAFE**: Replicate Research Data Safely
- **B2STAGE**: Get Data to Computation
- **B2FIND**: Find Research Data
- **B2HANDLE**: Register your Research Data
- **B2ACCESS**: Identity & Authorisation

**B2ACCESS**: Network of trust among authentication and authorization actors

**B2HANDLE**
- Identity
- Integrity
- Authenticity
- Locations

**B2SAFE**
- Data corruption and access optimization

**B2STAGE**
- Dynamic relocation to HPC workspace for processing

**B2FIND**
- Aggregated EUDAT metadata domain
- Data inventory

External community metadata store
What is General Data Protection Regulation*

- EU Regulation 2016/679 to
  - strengthen data protection for individuals within EU
  - addresses export of personal data outside the EU
- Enter directly into application 25 May 2018
- Data protection to be embedded in services
- The Individual has the right to
  - Be informed – informed consent
  - erasure
  - restrict processing
  - data portability
- GDPR has created plethora of consultants offering generic advice without much operational impact

* GDPR
Risks related to GDPR

- GDPR Sanctions
  - regular periodic data protection audits
  - a fine up to 10/20 MEUR or up to 2%/4% of turnover
- Lawsuits
- Uncertainty
- Delays
- Costs
- Loss of trust
- Cannot utilise Open Data
- Lost research opportunities
- Loosing data and data processing to non-EU players/major global cloud providers
No privacy without security

- The requirements of GDPR must not stay loose from development and service production.
- GDPR is an additional requirement for operational security and should be implemented according to well known best security practices.
- Without comprehensive operational security controls the requirements for responsibility, accountability and notifying of breaches cannot be duly implemented.
- Researches, research institutions, research infrastructures and data centers must provide reliable, automated and secure processes for consent, erasure and data portability.
- All this will require a considerable amount of development.
- Organisations should appoint a Data Protection Officer with close ties to operational security to monitor compliance with GDPR - focus on 'how', not only 'what'.
EUDAT Privacy Roadmap

- It is very important that research infrastructures & data centers develop efficient and feasible ways to implement GDPR.
- The most efficient way to achieve this is by sharing best security practices and related codes and processes.
- In EUDAT this GDPR will be implemented by:
  - Terms of Use and Privacy Policy
  - Operational privacy guideline
  - Privacy by design during service development
  - Hardening and ensuring access controls/logging
  - Cryptographic privacy controls
  - Privacy awareness training
  - Penetration and vulnerability testing
  - Procedures for consent, for data erasures and for data portability
- Great efficiency benefits in sharing policies, practices, procedures and code between research infrastructures.