Information Security, Open Data and the new EU Data Protection Regulation

Jan Wennström
Chief Information Security Officer
Åbo Akademi
7.3.2017
Information security in a nutshell

- **Identify the information** – and handle it correctly (i.e. according to laws and agreements) – If unclear: Ask Your boss (he/she will know or ask me)

- **Remember: Confidentiality, Integrity, Availability (CIA)**
  1. **Protect** Personally Identifiable Information (PII) and trade secrets agreed upon extremely carefully
     1. Encrypt PII if stored on removable media (and laptops)! (ask ICT-service for guidance)
     2. Remember to protect also the backup:s (physically, encrypted or both)
  2. **Store** your data so that only you/your group can access it (preferably your home-directory/a project folder on the pcinst-server)
  3. **Backup** your data (the pcinst-server is backed up automatically) (Ransomware and mistakes by users/programs are Real Threats)

- **When making Open Access:** Think through what You may publish and how
The new EU General Data Protection Regulation (GDPR)

- Emphasis on handling and management of personally identifiable information (PII)
  - Anonymization & pseudonymisation
  - New in GDPR: FINES! (maximum capped to millions of €)
- Especially the rights of the data subjects to:
  - Check what has been registered
  - Be informed about infringements
  - Be forgotten – there are however restrictions
  - Move information from one service provider to another
- **Remember to record processing activities!**
  https://survey.abo.fi/lomakkeet/8622/lomake.html