Taking Privacy Laws into Account in Service Development

13th Fruct Conference , 26.4.2013,
Petrozavodsk, Russia

Dr. Pekka Jäppinen
Lappeenranta University of Technology

Open your mind. LUT.
Lappeenranta University of Technology

Open your mind. LUT.
Lappeenranta University of Technology

Structure of presentation

- Privacy
- European union view on privacy
- Meaning of laws from developer perspective
- Service developer perspective
- Summary

Open your mind. LUT.
Lappeenranta University of Technology

Privacy

- Privacy is a right for control about the use and transfer of information about yourself.
- Sensitiveness of data is dependent on the person, the culture and time.
- Protected by laws and regulations
  - Determines how personal data
    - **can be used** and **must be protected**
  - Differ vastly between different countries in the world
- Privacy preservation is important for upkeeping users trust

Open your mind. LUT.
Lappeenranta University of Technology

EU and Privacy

- EU acknowledges that you have all the rights to the information about you.
  - User consent required for use
  - EU legislations regarding personal data use: http://ec.europa.eu/justice/data-protection/index_en.htm
- Commission is working on the new regulation about protection of personal data
  - The protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation): http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Open your mind. LUT.
Lappeenranta University of Technology

Some points from regulation draft

- Data protection by design and by default
  - Privacy by design, Privacy by default
- Personal data controller responsibilities described in article 22 include:
  - Adopt policies and implement appropriate measures to ensure personal data is handled properly
  - Implement mechanisms to ensure the verification of the effectiveness of the measures
  - Be able to demonstrate that the situation is so.
- Bigger companies have to have designated person that is responsible for privacy

Open your mind. LUT.
Lappeenranta University of Technology

Potential impact of new regulation?

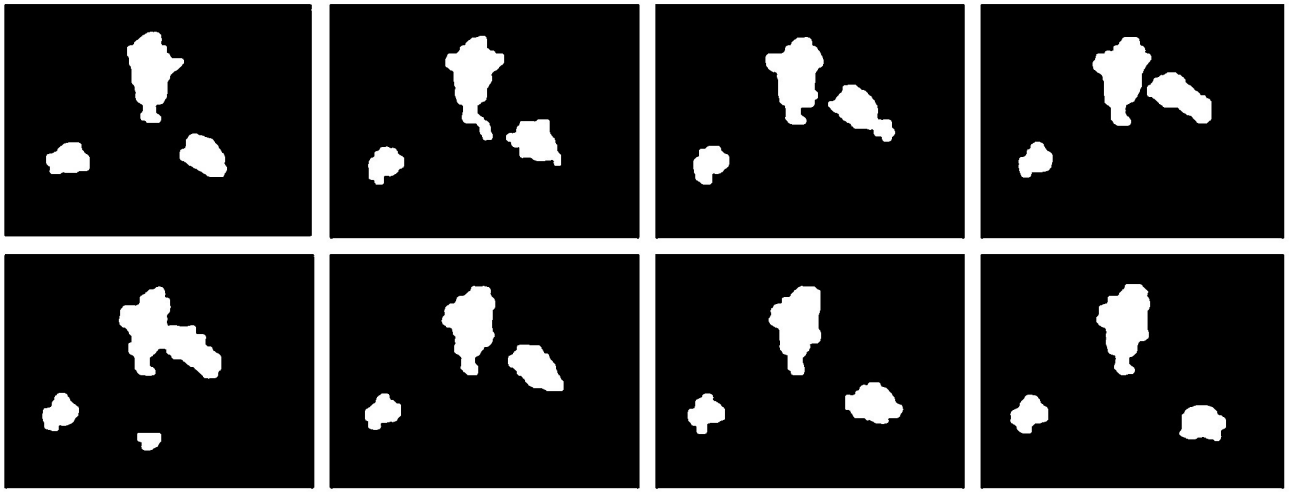
- Privacy by design principle adopted
- Methods for analysing privacy risks against IT solutions will be developed.
- Developers need to be able to demonstrate that their software will not leak private information?
- Personal information use need to be justified even more?

Taking privacy into account

- Avoid relying totally on the use of personal data
  - Allow service users to decide whether they want their data to be used for e.g. personalisation
  - Service providers should gather only the personal data that is needed → enable configuration for the type of data gathered.
- Think about the data granularity
  - e.g. Daily electricity consumption vs real time consumption data.

Open your mind. LUT.
Lappeenranta University of Technology

- Differentiate identity from the other data when possible
  - Anonymise when possible
    - Personalisation needs preferences not identities
  - e.g. images below from Mobiserv project (courtesy of Dr. Anastasios Tefas, University of Thessaloniki)



- Storage
  - Temporary or longterm storage
  - Remove old data that is not needed.
  - Encrypt the stored data
- Support access control
  - Internal
    - Access only to software components that need the access
  - External
    - Personnel access

Open your mind. LUT.
Lappeenranta University of Technology

Privacy research at LUT

- Privacy threat analysis
  - Smart Energy Grids
  - Independent living support system, Mobiserv
- Privacy risk analysis method development
- ME 2.0
  - Personal information management system that
  - Enables privacy preserving ubiquitous service personalisation.

Open your mind. LUT.
Lappeenranta University of Technology

Summary

- Protecting privacy is important for
  - system acceptability and upkeep of user trust.
- Laws and regulations determine the minimum required effort
  - It is important to understand the basic laws of your market area

Open your mind. LUT.
Lappeenranta University of Technology

- Privacy can be best protected by following privacy by design principle
  - Think what information is needed
  - Do not store anything longer than needed
  - Anonymise stored data
  - Control access to the stored data