Digital Defence

Developing privacy-compliant sofware and selling it to the legal department

Ot van Daalen

GOTO Amsterdam 2015 – 19 June 2015

About me

- Founder of privacy law boutique
- Lecturer at Institute for Information law
- Founder of Bits of Freedom
- Nerd / programmer

Goals

- Understand the risks involved in privacy law
- Understand the basic rules
- Develop privacy-compliant software
- Convince the legal department

Privacy infringements carry serious risks

- Damage to reputation
- Redesign of software or processes
- Administrative proceedings (legal costs)
- Fines (up to 2% of worldwide turnover?)

European privacy rules require transparency and care

- Provide information on what you do
- Limit use of personal data
- Minimise collection, retention and access of personal data
- Reading and writing to users devices requires consent
- Secure personal data

Provide information on what you do

- Specific information
- On identity, purposes, data, etc.
- Layered information if complex
- Avoid legalese
- Be creative, involve the UI/UX dept!

Limit use of personal data

- Data needs to be collected for a specific purpose
- Use only allowed if compatible with initial collection
- Data may only be used if there is a basis
- This usually requires (i) consent or (ii) balancing of interests
- So: determine purpose and determine basis

Obtain true consent

- Consent needs to be specific, free and informed
- Terms and conditions usually don't cut it
- Provide context specific buttons
- Be specific and informative

Or balance the interests

- This involves a discussion with the legal department
- Developers should focus on safeguards to minimise the privacy impact:
  - Minimise data collection (see also later)
  - Offer opt-out possibilities
  - Use hashing, chinese walls
  - Offer data portability

Reading and writing to users devices requires consent

- In order to protect against malware, EU legislator introduced RW-protections for user devices
- Affects analytics cookies, transferring address books, etc.
- Especially for apps, be specific, informed, explain what you do, provide opt-out if necessary

Secure personal data

- Required to take technical and organisational measures to secure personal data
- This means security measures in the backend, frond, but also in user devices (to a certain extent)
- Encrypt: all user data over the internet, possibly on the device
- Hash: passwords, identification mechanisms, user data (note that this is not anonymisation, just pseudonymisation)
- Also: patching, logging, auditing...
- And be prepared for a data breach

Convince the legal department

- Explain you're providing the necessary information and obtaining specific consent
- Explain you've checked whether the data processing is proportionate and whether there are less infringing options
- Explain which safeguards you've taken to minimise privacy infringement, including opt-out, hashing

Questions?

Ot van Daalen

+31 6 5438 6680

ot.vandaalen@digitaldefence.net

@digidefence

Digital Defence