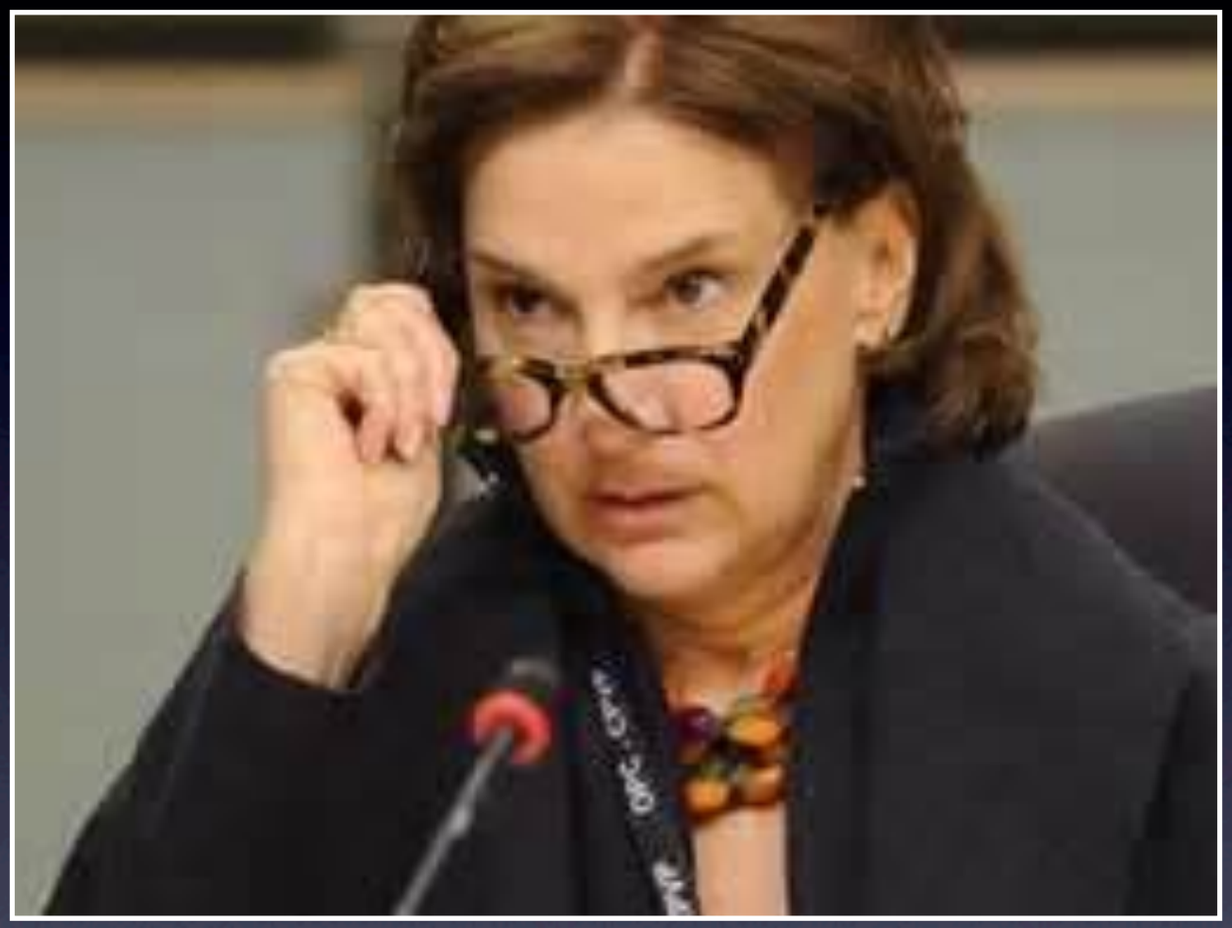
EU Privacy Regulation Update

Dr. Ville Oksanen 18.10.2013

Who's talking..

- L.LM. , Ph.D. (Technology law)
- At TKK (Aalto) since 2001
- At Helsinki University since 2009
- Partner, Turre Legal
- Founder, Electronic Frontier Finland
  - Currently Vice Chairman
- Blogger - "Lex Oksanen"



Privacy regulation updata

Original goal

- To update the existing regulation to meet the change in technologies
- To give more rights to both citizens and also data protection authorities

However..

- “Regulatory capture” in action
- Heavy lobbying from e.g.
  - U.S Government
  - Facebook, Google etc.
- To water down the proposal

Key features

- “Clarified definitions of “personal information” and “consent”.
- Data protection by Design
- Accountability + Notification of breaches
- Portability + right to access (for free)
- Right to be forgotten
- International regulatory scope?

Personal information

- A person must be considered identifiable when either the data controller or another natural or legal person can identify the person.

Consent

Data subject's perceived behaviour

or

Result of an active choice

Data protection by Design

Article 23:
"The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

Right to be forgotten

- Most controversial feature
- Many open questions
  - Practical (backups? Who pays the costs)
  - Content spesific (photographs? Discussions?)
- Application to data given to 3rd parties`

Accountability

Article 22
"The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors."

Notifications

- Article 31:
  "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours."

- Article 32:
  "When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay."

Portability

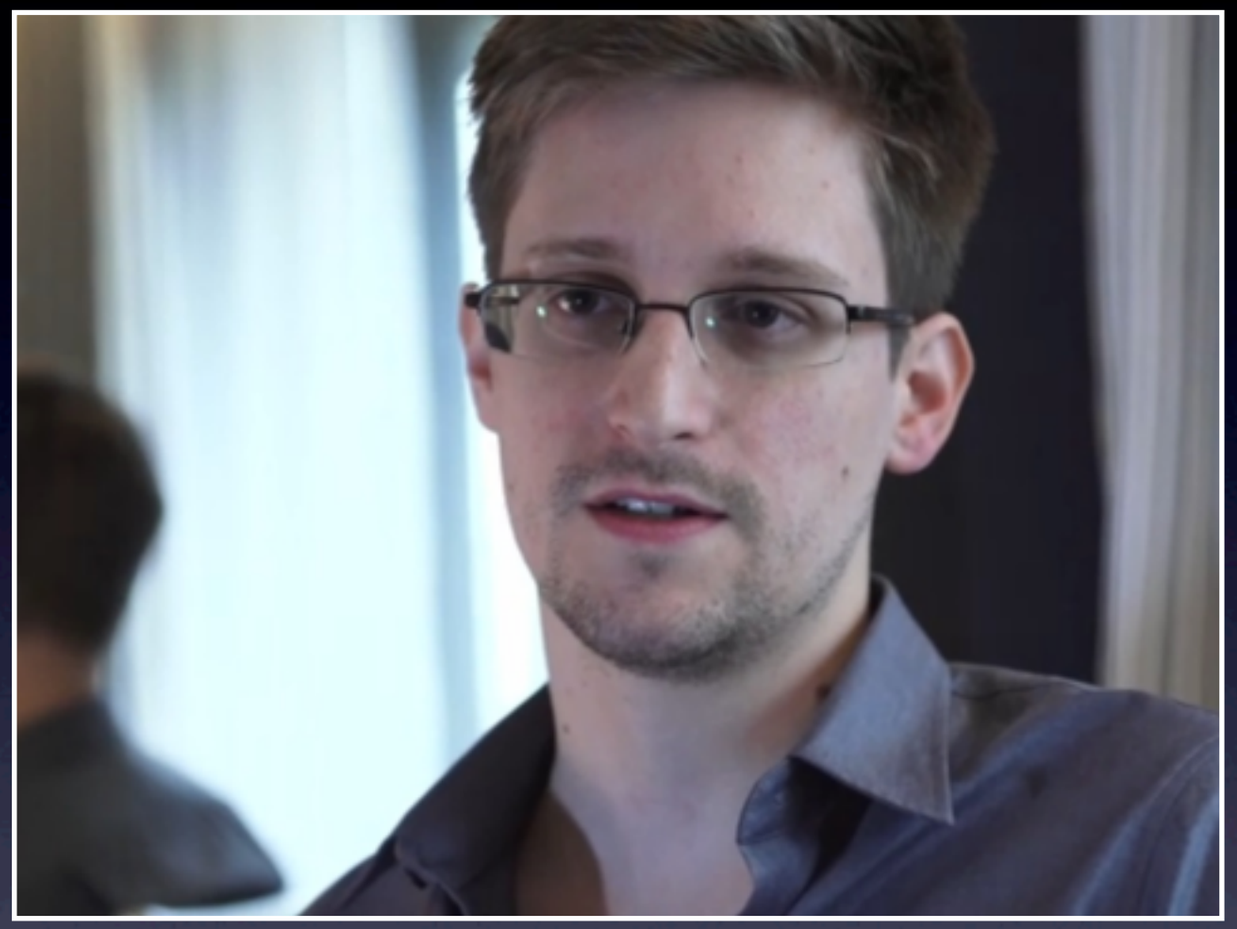
Data portability

Article 18
"The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject."

International scope

- A change from a general prohibition of transferring data to third countries (notwithstanding derogations) as contained in the Directive to the principle that transfers can only take place if enumerated conditions are met
- Fines - %

Current State?



Case Snowden

Amendments Dossier

4867	2012/0011(COD) Personal data protection: processing and free movement of data (General Data Protection Regulation) 2012/08/11 IMCO 373 amendments... source: PE-500.411 2012/11/29 JURI 380 amendments... source: PE-500.695 2012/12/20 ITRE 192 amendments... source: PE-502.053 2012/12/21 ITRE 561 amendments... source: PE-502.055 2013/01/16 LIBE, LIBE 350 amendments... source: PE-501.927 2013/03/04 LIBE 838 amendments... source: PE-504.340 2013/03/06 LIBE 1762 amendments... source: PE-506.168 2013/03/08 LIBE 183 amendments... source: PE-506.173 2013/09/01 ITRE 228 amendments... source: PE-502.174

'Breakthrough' on data protection bill

17.10.13 @ 20:54

RELATED › US spy scandal prompts redraft of EU data bill › Parliament endorses controversial EU flight rules › MEPs approve disputed tobacco law

BY NIKOLAJ NIELSEN

BRUSSELS - After eighteen months of intense negotiations, MEPs spearheading the European Data Protection regulation have reached a compromise.

(http://euobserver.com/justice/121817)

Article 83a
Processing of personal data by archive services

1. Once the initial processing for which they were collected has been completed, personal data may be processed by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest, in particular in order to substantiate individuals' rights or for historical, statistical or scientific research purposes. These tasks shall be carried out in accordance with the rules laid down by Member States concerning access to and the release and dissemination of administrative or archive documents and in accordance with the rules set out in this Regulation, specifically with regard to consent and the right to object.

2. Each Member State shall notify to the Commission provisions of its law which it adopts pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 83
Processing for historical, statistical and scientific research purposes

1. ***In accordance with the rules set out in this Regulation***, personal data may be processed for historical, statistical or scientific research purposes only if:

(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;

(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information ~~***as long as these purposes can be fulfilled in this manner***~~ ***under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects.***

Level of consent?

But a source close to the file told this website that it is up to the company to determine the balance of what is in the consumer's 'legitimate interest' and their own rather than having to seek out consent.

A company that sells a car, for instance, can then pass on direct marketing materials to the client on other products without asking.

EduGain

- Categories:
  - category PII: the Service Provider processes personal data
  - category non-PII: the Service Provider processes no personal data
- Attributes such as end user's full name (cn), email address (mail) and unique 302 identifier (eduPersonPrincipalName) are personal data.

Questions?

Comments?

ville.oksanen@aalto.fi-- twitter: villoks