CHALMERS UNIVERSITY OF TECHNOLOGY | UNIVERSITY OF GOTHENBURG

Compliance-by-Construction ?

Privacy Compliance via Model Transformations

T. Antignac, R. Scandariato, G. Schneider

Riccardo Scandariato

Software Engineering Division
Chalmers | University of Gothenburg

riccardo.scandariato@cse.gu.se

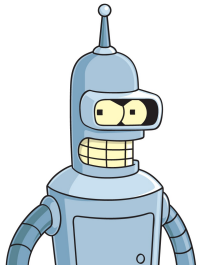
www.scandariato.org

HoliSec
Holistic Security of Connected Vehicles

GDPR challenges…

…that we often discuss with industrial parners

- What does it mean?
  (for technical ppl)
  - How do find we are not in compliance?
  - How do we fix a non-compliance issue?



vs

- Lack of privacy experts

- Large-scale systems (micro-services, IoT…)

Technical compliance to GDPR

At the level of design models

- Model-based (**PA-DFD**), automated

- Recipe
  - **Where**: Identify hotspots
  - **What**: Apply model transformations
  - **Why**: Proven privacy properties

T. Antignac, R. Scandariato, G. Schneider, **A Privacy-Aware Conceptual Model for Handling Personal Data**, ISoLA 2016

This paper

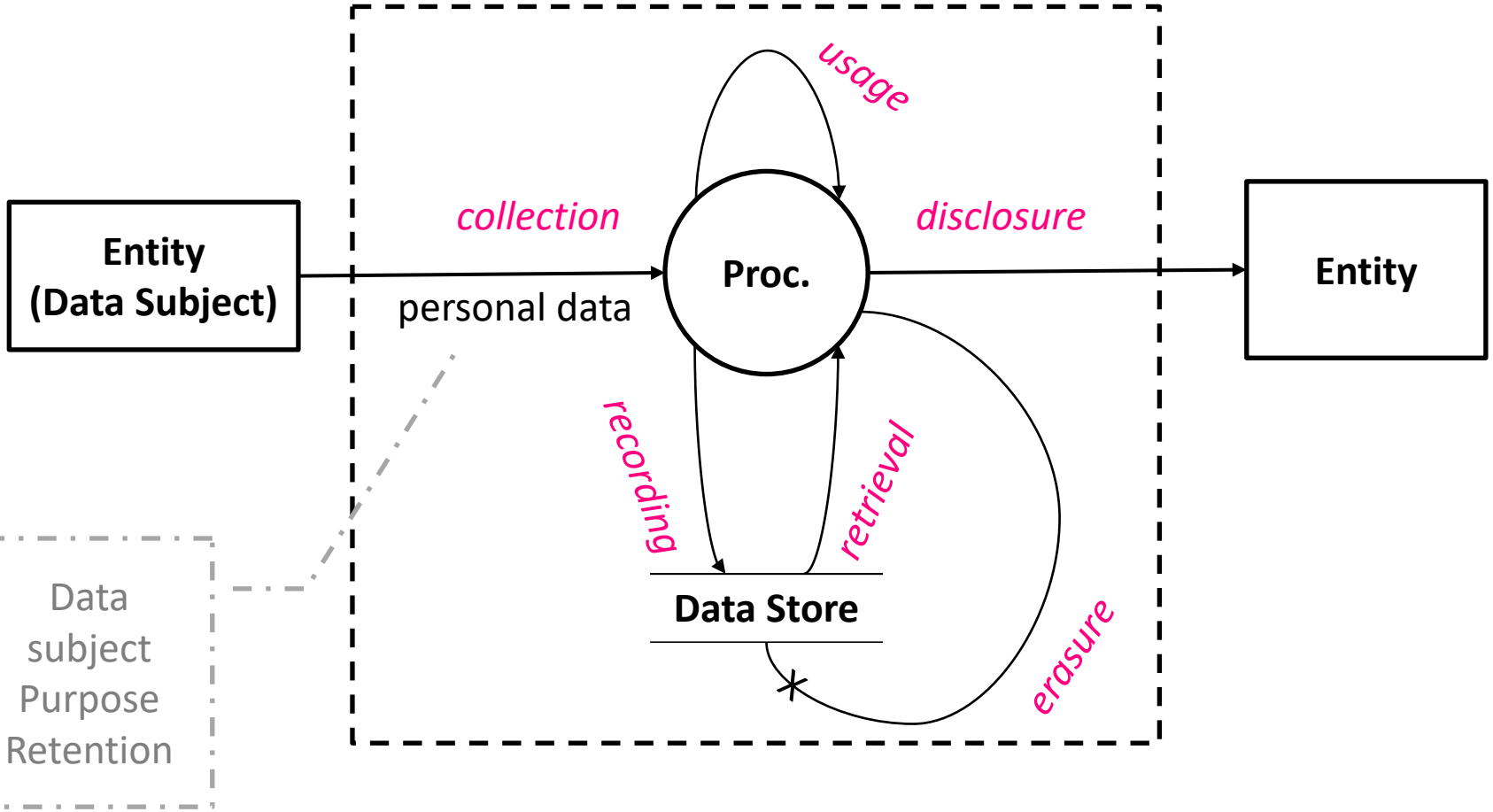
Next paper ;)

Privacy principles

- Purpose limitation
- Retention time
- Accountability of data controller
- Right to erasure

Hotspots in a PA-DFD

A.k.a. interactions

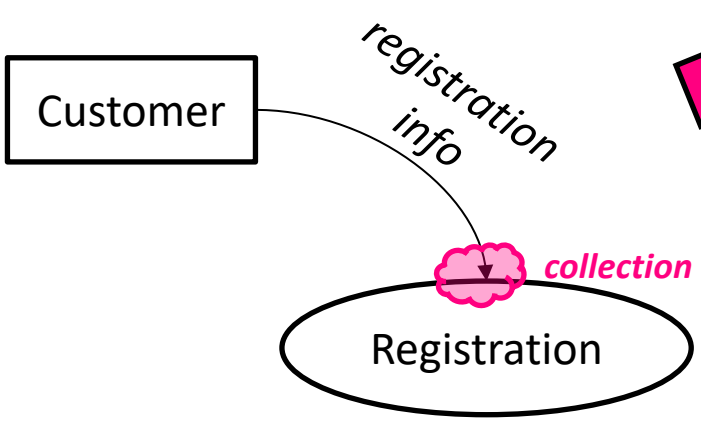


Constructive approach to GDPR compliance

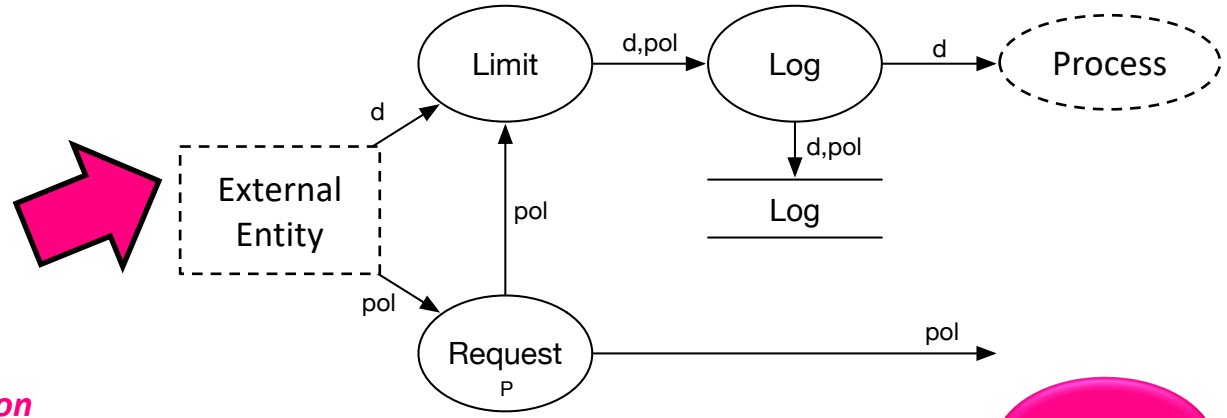
Towards proven model transformations

Hotspots (where)

Privacy-sensitive part of the design model



Transformations (what)



WiP

Proof

1. Transformed model is *well-formed*
2. *Functionality* is preserved
3. *Privacy properties* hold:
   - ✓ Purpose limitation
   - ✓ Accountability of data controller
   - ✓ Data subject's right to change

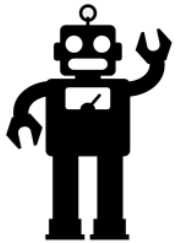
TLDR ;)

Technical definition of (GDPR) compliance @ design

(I know, I know… it's not the entire GDPR)

Automation for compliance-by-construction

(yes, yes… the model might become a mess)



Questions ?

riccardo.scandariato@cse.gu.se

www.scandariato.org