Eclipse Foundation Working Group: Privacy-by-Model community

Antonio Kung (TRIALOG) antonio.kung@trialog.com
Yod Samuel Martin (UPM) ys.martin@upm.es
Philippe Krief (Eclipse Foundation) philippe.krief@eclipse-foundation.org

Methods and Tools for GDPR Compliance through Privacy and Data Protection 4 Engineering
Should privacy regulations be an engineer’s job? (Tip: It seems it should indeed)

What Developers and Publishers Need to Know About the GDPR

Heather Burns is a digital law specialist in Glasgow, Scotland. Her focus is researching, writing, and giving talks about internet laws and policies which impact... about Heather...

How GDPR Will Change The Way You Develop

IEEE POSITION STATEMENT
In Support of Privacy Engineering

Adopted by the
IEEE Board of Directors
18 November 2018

Private matters
15 steps to developing GDPR-compliant apps

Your Guide to the GDPR
Here’s what you need to about the EU’s General Data Protection Regulation, which goes into effect
25 May 2018

I’m a Developer and General Data Protection Regulation (GDPR) is no big deal. Or is it?

Bryan Solis
Technical Evangelist at @Kentico. @Microsoft MVP. Husband. Speaker. Father. Grandfather. Mediocre bowler. Available for a beer.
Dec 6, 2017 - 8 min read
PDP4E response: what engineers need

“Endow engineers with privacy and data protection tools aligned to their mindset”
Model engineering
constructing proportionally-scaled miniature **working** representations of full-sized machines

Model driven engineering
expressing specifications through **processable** models.
Diagram orientation (e.g. UML)
Complementary modelling views and disciplines for privacy engineering

Requirements Models:
- Privacy goals and properties
- Regulations (GDPR): principles, rights, obligations, measures
- Standards (ISO29100) ... in the context of functional reqs.

Assets model:
- What do we need to protect? (personal information, human rights, biz. reputation...)

Threats model:
- What from?

Controls model:
- How do we protect them?
- How do we know others protect them as well?

Reference framework model:
- What activities are mandated?
- Who shall carry them out?
- What artifacts shall be produced?

Structural (data) model e.g.
- which data is personal?
- is it sensitive?
- what is the basis for collection?

Procedural (dataflow) model e.g.
- which processes deal with personal data?
- which processing operations it is being subject to?
- which data flows between operations?
- for what purpose it is being used?
- who is authorized to access that data?

Architectural (deployment) model
- who stores and processes data?
- under which jurisdiction?

Assurance case:
- How can I argument that I’m compliant?
- Which evidences do I have to prove that?

Method engineering

System analysis & iterative design

References
Method and functional integration
Model-based engineering is well established

- **Communities**
  - OMG - 1989 (UML, BPMN, SysML)
  - Incose – 1990 (body of knowledge)

- **Some URLs**
  - https://www.sebokwiki.org/

- **Some references**
  - Model driven development. IEEE so
  - Model-based systems engineering: systems, man and cybernetics. Jan

- **Standard under development**
  - ISO/IEC 24641 Model-based system
Model-based privacy engineering lifecycle? (a.k.a. “Can we Dare we share & reuse models?”)

- Define modelling language
- Model regulatory constraints
- Tailor model to context
- Instantiate model in project
- Transform models to comply
- Validate transformed model

Project-independent

Knowledgebases

Industry policies

Patterns

Supply-chain validation

Biz. context

Sys. models

Project-specific
Application Privacy Protection Models

- Consumer applications Protection models
- Data processing Protection models
- IoT applications Protection models

- Health
- Social network
- Mobility
- Smart home
- Fintech
- Connected vehicles
- Smart energy
- E-mobility
- Assisted Living
- Security
- ...
Privacy Engineering Project Models

**Framework Models**
- Cyber security framework
  - ISO/IEC 27110
- NIST privacy framework

**Risk Management Models**
- Threat model
  - STRIDE
- Control model
  - ISO/IEC 27001, 27701

**Privacy operationalisation methods Models**
- Security and privacy principles
  - ISO/IEC 29100
- Design strategies
  - ISO/IEC 27550
- Privacy capabilities taxonomy
  - ISO/IEC 27561 (POMME)

**Assurance Models**
- Profiles
  - NIST
- Evidence
- Assurance process

---

Open Research Webinars – March 3, 2021
Eclipse Privacy Protection Community (proposal)

**Stakeholders**
- **Privacy model expert** PbM
- **Steering committee**

(1) Provides Guidance for models
(2) Uses

**Stakeholders**
- Application privacy protection Task force

(3) Provides model

**Stakeholders**
- Privacy engineering project Task force

(3) Provides model

**Stakeholders**
- Application privacy protection Task force

(3) Provides model

(4) Validates model

**Stakeholders**
- Privacy model expert PbM
- **Validation committee**

(4) Validates model

(5) Publishes model

Models
The way forward

● Initial projects
  ○ Application privacy
    ■ C-ITS,
    ■ Smart grid data exchange
  ○ Privacy engineering
    ■ Risk analysis
    ■ Requirements engineering
    ■ Privacy-by-design
    ■ Assurance

● Community participants
  ○ Eclipse foundation
  ○ PDP4E partners

● Other potential participants
  ○ Ann Cavoukian
  ○ KU Leuven
  ○ NIST
  ○ U.Ulm
  ○ Data space stakeholders
  ○ H2020 competence networks

● Other potential applications
  ○ Fintech
Methods and Tools for GDPR Compliance through Privacy and Data Protection 4 Engineering

Community @ Eclipse Foundation
eclip.se/h0

Contacts to join the community:
Antonio Kung antonio.kung@trialog.com
Samuel Martin ys.martin@upm.es
Philippe Krief philippe.krief@eclipse-foundation.org

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 787034

www.pdp4e-project.eu
@PDP4E
linkedin.com/company/pdp4e-project/
yt.vu/+pdp4e

Open Research Webinars – March 3, 2021