Methods and Tools for GDPR Compliance through Privacy and Data Protection 4 Engineering

PDP4E privacy engineering toolkit

Yod Samuel Martín (UPM)
Gabriel Pedroza (CEA LIST)

IPEN Workshop 2019 - Rome, June 12 2019

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 787034
Should GDPR be an engineer’s job?
(Tip: It seems it should indeed)

What Developers and Publishers Need to Know About the GDPR

How GDPR Will Change The Way You Develop

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

15 steps to developing GDPR-compliant apps
The privacy and data protection engineering gap

What engineers get...

- GDPR
- PbD

What engineers want...

- PETs
- PPM/PEM
PDP4E response: what engineers need

“Endow engineers with privacy and data protection tools aligned to their mindset”

- Engineers are not privacy experts, yet they will face privacy issues (even if they may get expert advice)
- Privacy adoption entails for methods and tools integrated within the large heritage of sw. & sys. engineering
  1. Seamlessly include privacy & data protection into software & system engineering tools
  2. Integrate privacy & data protection activities into the SDLC stages
  3. Provide a readily available body of knowledge with existent wisdom
  4. Foster a community of privacy & data protection engineering
PDP4E response: what engineers need

- Knowledge Bases
- Metamodels
- Requirements engineering
- Model-driven design
- Risk management
- Software and Systems Engineering Disciplines
- Privacy and Data Protection Methods
- Existent Privacy & Data Protection Methods
- Model-driven design
- Assurance and certification
- Smart grid demonstrator
- Connected vehicle demonstrator
Even if there is no damage to the data subject, you are not compliant if you don’t assess and mitigate risks.

Multilateral risk management:
- Data protection impact assessment
- Security impact analysis, security measures
- Compensations, liabilities and fines
- Supply Chain and Vendor Relationship Management (i.e. processors’, joint controllers, third parties, transfers...)
- Risks to rights and freedoms of the data subjects
- Risks derived from data breaches
- Derived business risks
- ...

But not everything in GDPR is a risk:
- e.g. “risk of not asking the data subjects their age” ✗GOAL
- e.g. “risk of not providing a transparent policy” ✗GOAL
- vs “risk of misidentifying a child as an adult” ✓UNCERTAINTY
- vs “risk of users having low reading skills” ✓UNCERTAINTY
MUSA risk management tool for security impact assessment
GDPR modelling in OpenCert: Reference Framework and Assurance Patterns
Papyrus overview

- UML model explorer
- Editors for all UML diagrams
- Form-based properties edition
Privacy & data protection requirements metamodel (through Papyrus)
Modelling-driven design for Privacy and Data Protection engineering (through Papyrus)

- Personal data detector
- Data Diagrams (SQL+UML class)
- Process Diagrams (DFD \rightarrow BPMN/UML Activity)
- Architecture Diagram
  - (UML composite / SysML BDD/IBD)

- Code verification and validation
- Model transformation
- Evidences (traceability, V&V...)
- Systems Assurance
- Privacy Controls
- System (Asset) models
- Risk Management
- Requirements Engineering
- Requirements (GDPR, ISO29100)

24/06/2019
Privacy & data protection model-driven design. method

1) Choose design strategy to fulfill goals/requirements

2) Design/enrich system Process view(s)

3) Apply strategy (e.g., inform, control, enforce, demonstrate)

24/06/2019

PDP4E
Image sources

- Slides 1, 2, 5: all the logos of the PDP4E partners, publications, and others are copyrighted and/or trademarked by the respective organizations.

- Slide 2: captures of the headlines from browsing through the following webpages, used under right of quotation:
  - What Developers and Publishers Need to Know About the GDPR [https://medium.com/struucom/what-developers-and-publishers-need-to-know-about-the-gdpr-cfe0f97412f](https://medium.com/struucom/what-developers-and-publishers-need-to-know-about-the-gdpr-cfe0f97412f) by Struu blog on Medium.
  - I’m a Developer and General Data Protection Regulation (GDPR) is no big deal. Or is it? [https://hackernoon.com/im-a-developer-and-general-data-protection-regulation-gdpr-is-no-big-deal-or-is-it-2f2b7b3f124](https://hackernoon.com/im-a-developer-and-general-data-protection-regulation-gdpr-is-no-big-deal-or-is-it-2f2b7b3f124) by Bryan Solis, at Hackernoon blog on Medium.

- Slides 3, 10 (images here cited under right of quotation or provided by PDP4E partners, unless otherwise specified):
  - Privacy by Design 7 principles [http://privacybydesign.ca/](http://privacybydesign.ca/) (offline) by Ann Cavoukian


- Slide 13:
  - DFD by Howard, M., & Lipner, S. (2006). The security development lifecycle : SDL, a process for developing demonstrably more secure software., p.113
  - Class diagram [https://www.flickr.com/photos/79364035@N04/8402807365](https://www.flickr.com/photos/79364035@N04/8402807365) by elisa_abuyah licensed under CC-BY--2.0 license [https://creativecommons.org/licenses/by/2.0/](https://creativecommons.org/licenses/by/2.0/)
Methods and Tools for GDPR Compliance through Privacy and Data Protection 4 Engineering

Thank you for your attention

Questions?

For more information, visit: www.pdp4e-project.org
We’ll be waiting for you at the APF exhibition booth!

Yod Samuel Martín (UPM)
ys.martin@upm.es

Gabriel Pedroza (CEA)
gabriel.pedroza@cea.fr