PDP4E

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)

SMASHING MAGAZINE

ABOUT THE AUTHOR

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

FEBRUARY 27, 2018 • 47 COMMENTS

How GDPR Will Change The Way You Develop

Privacy 4 # Security 38

STRUU Follow
The Expression Assistant
Feb 21 · 7 min read

What Developers and Publishers Need to Know About the GDPR

TechBeacon

Private matters

15 steps to developing GDPR-compliant apps

RESOURCES_AT WORK

WHAT YOU NEED TO KNOW ABOUT EUROPE'S DATA PRIVACY RULES

NEW GDPR REGULATIONS ON PERSONAL DATA WILL AFFECT EVEN INDIVIDUAL CODERS

Your Guide to the GDPR

Here's what you need to know about the EU's General Data Protection Regulation, which goes into effect 25 May 2018

By Rosa Maria Garcia Sanz

Bryan Soltis Follow
Technical Evangelist at @Kentico. @Microsoft MVP, Husband. Speaker. Father. Grandfather. Mediocre bowler. Available for a beer.
Dec 6, 2017 · 8 min read

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

The privacy and data protection engineering gap

What engineers get…

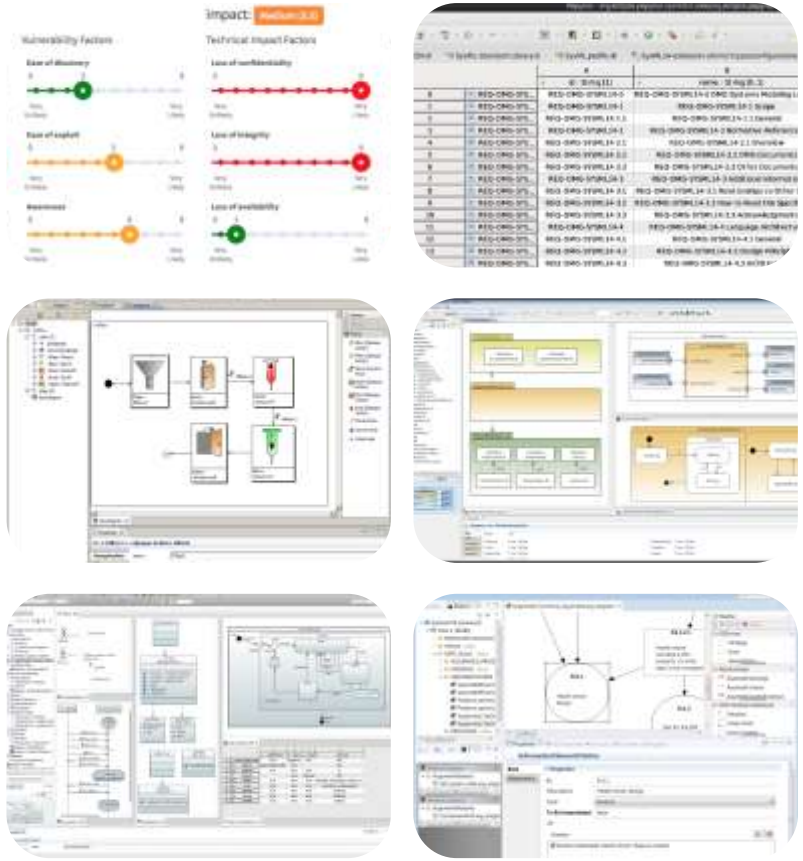
GDPR

PbD

PETs

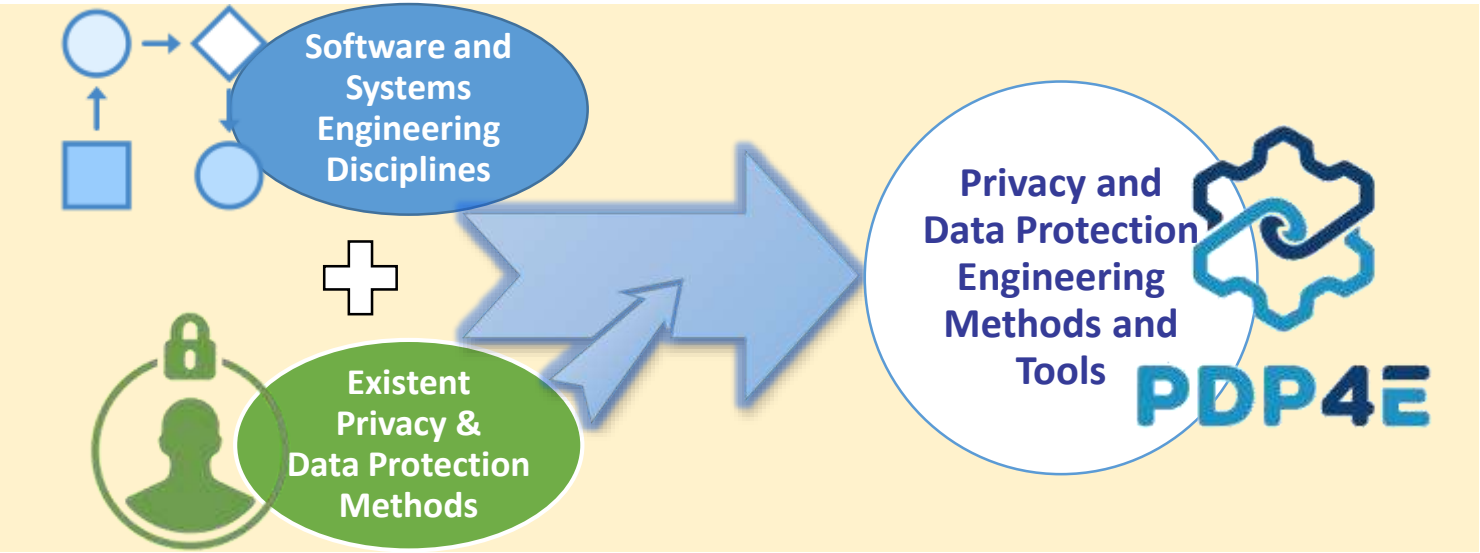
PPM/PEM

What engineers want…



PDP4E response: what engineers need

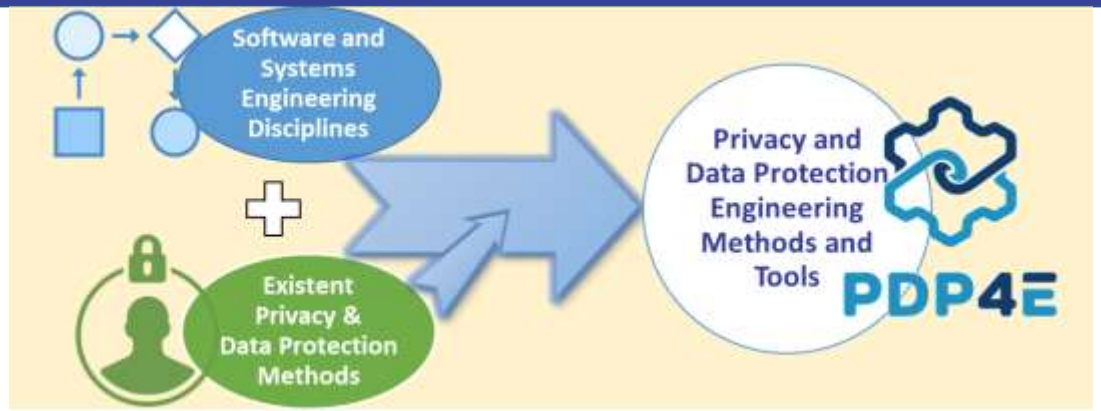
"Endow engineers with privacy and data protection tools aligned to their mindset"



- 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



Byproducts

TRL6

TRL7

Knowledge Bases

Metamodels

Requirements engineering

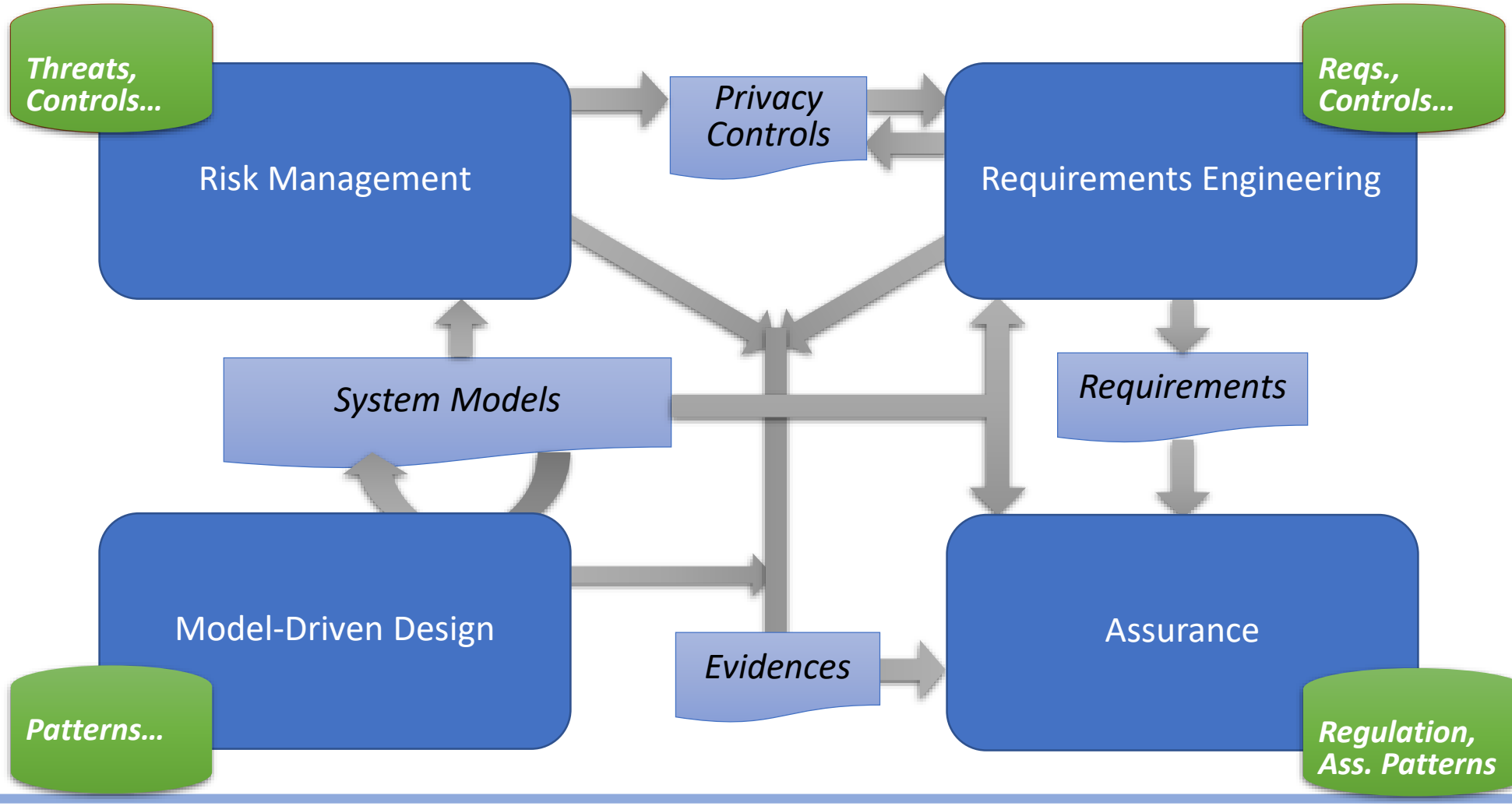
Model-driven design

Assurance and certification

Risk management

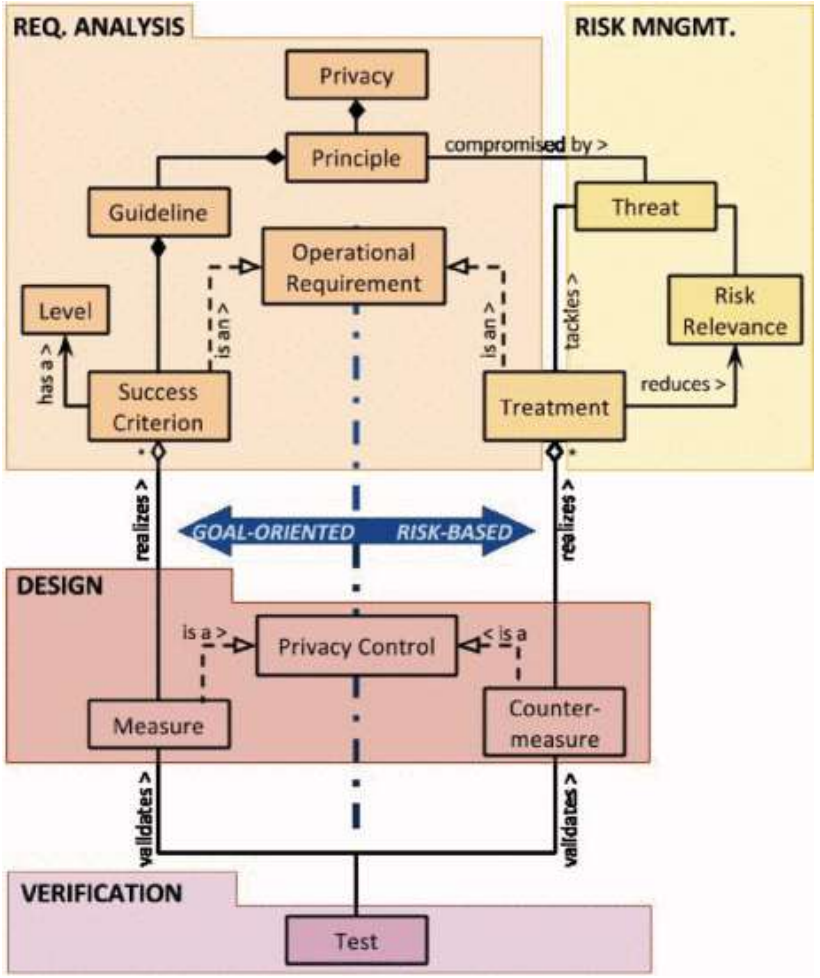
Smart grid demonstrator

Connected vehicle demonstrator

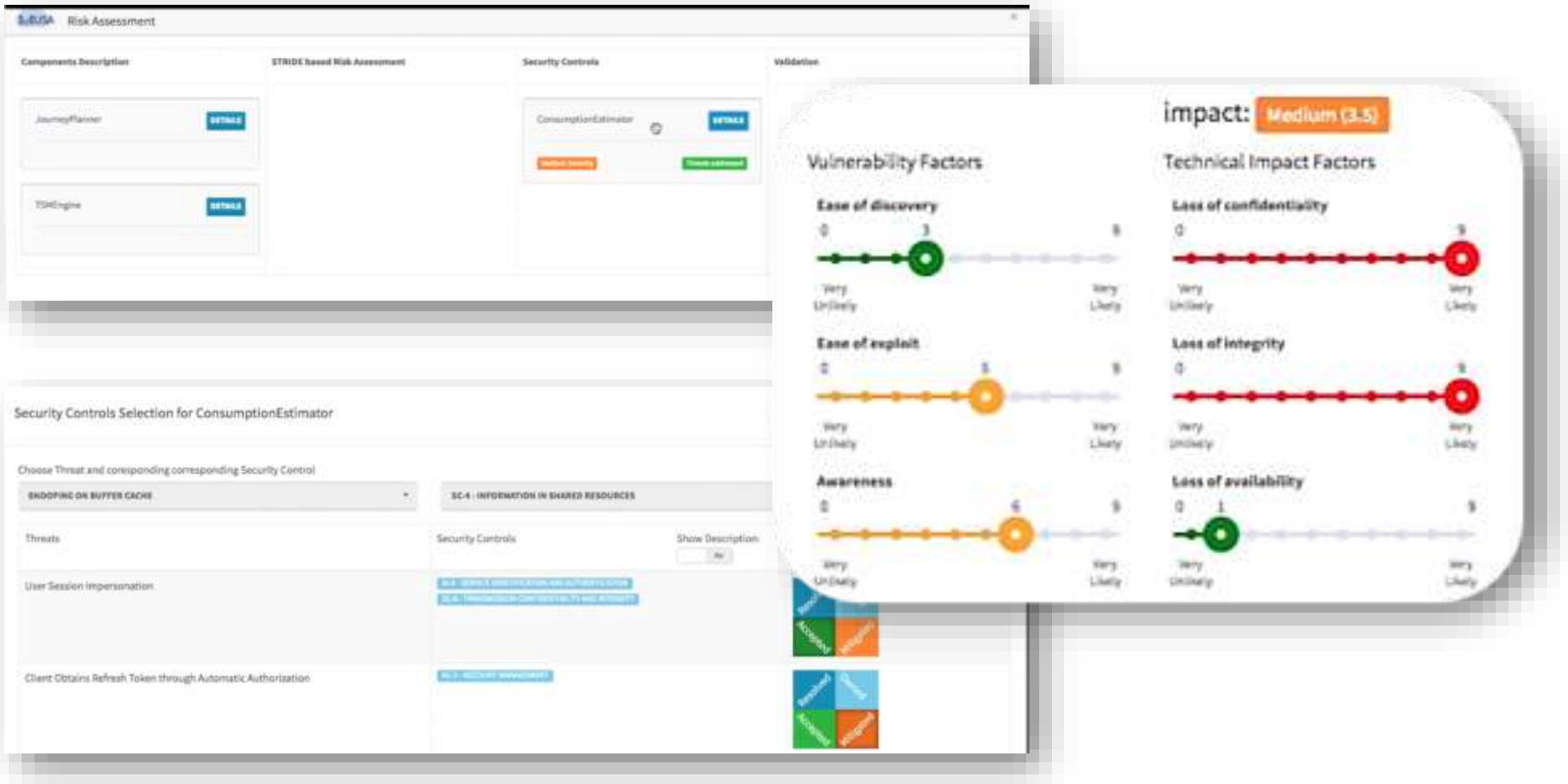

Threats, Controls…
Risk Management
Privacy Controls
Reqs., Controls…
Requirements Engineering
System Models
Requirements
Model-Driven Design
Evidences
Assurance
Patterns…
Regulation, Ass. Patterns

Risk-orientation of GDPR

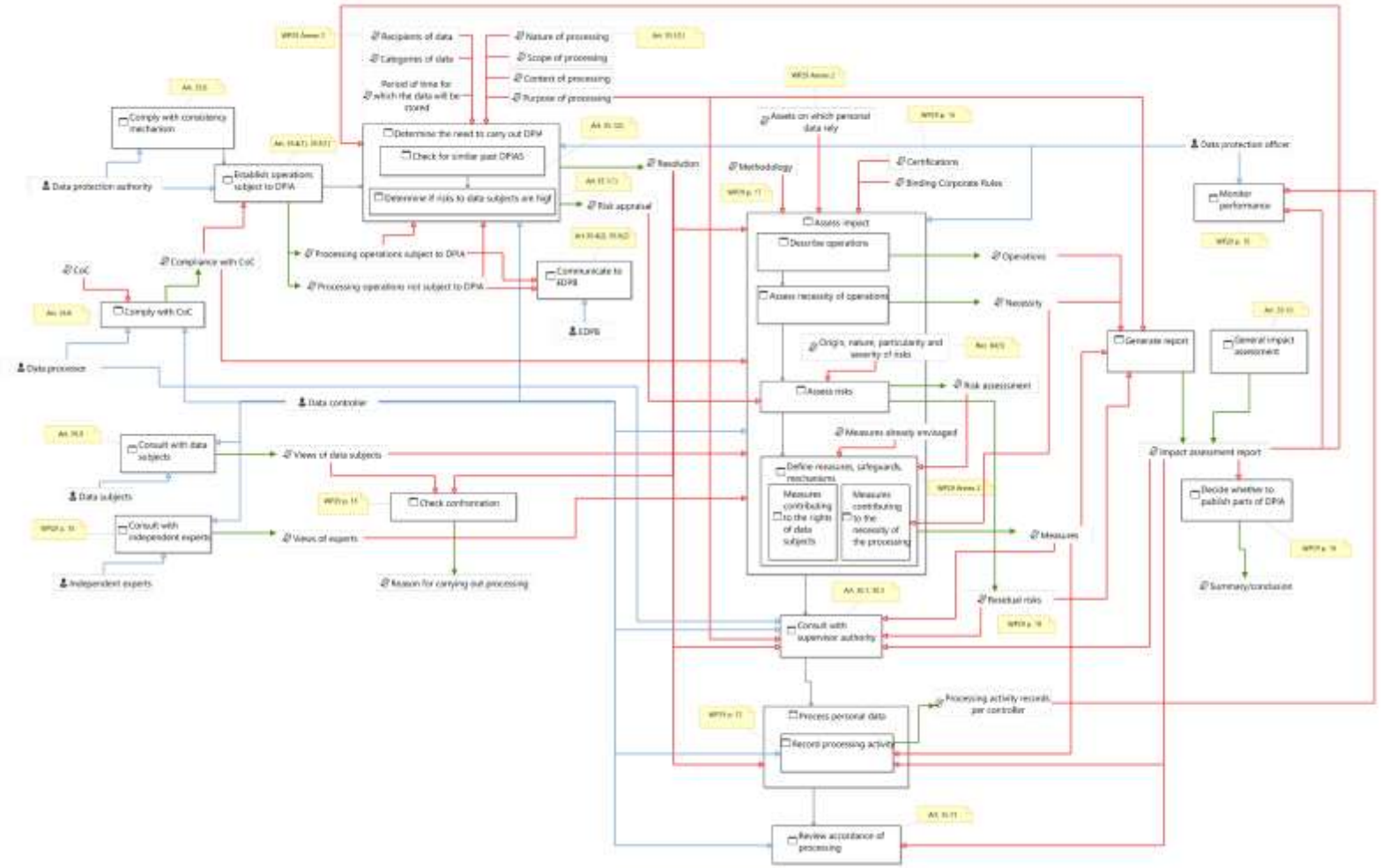
- Even if there is no damage to the data subject, you are not compliant if you don't assess and mitigate risks.
- Multilateral risk management:
  - ❑Data protection impact assessment
  - ❑Security impact analysis, security measures
  - ❑Compensations, liabilities and fines
  - ❑Supply Chain and Vendor 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 poilcy~~" ✘GOAL
  - vs "risk of misidentifying a child as an adult" ✓UNCERTAINTY
  - vs "risk of users having low reading skills" ✓UNCERTAINTY

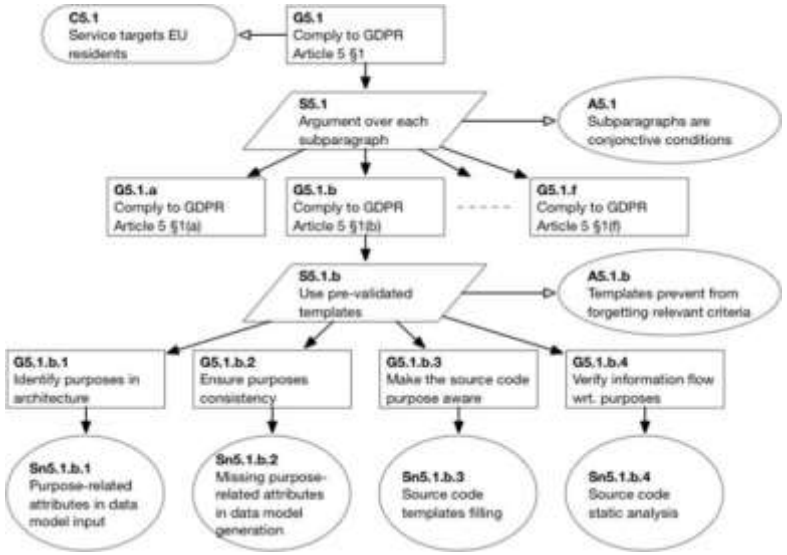


MUSA risk management tool for security impact assessment

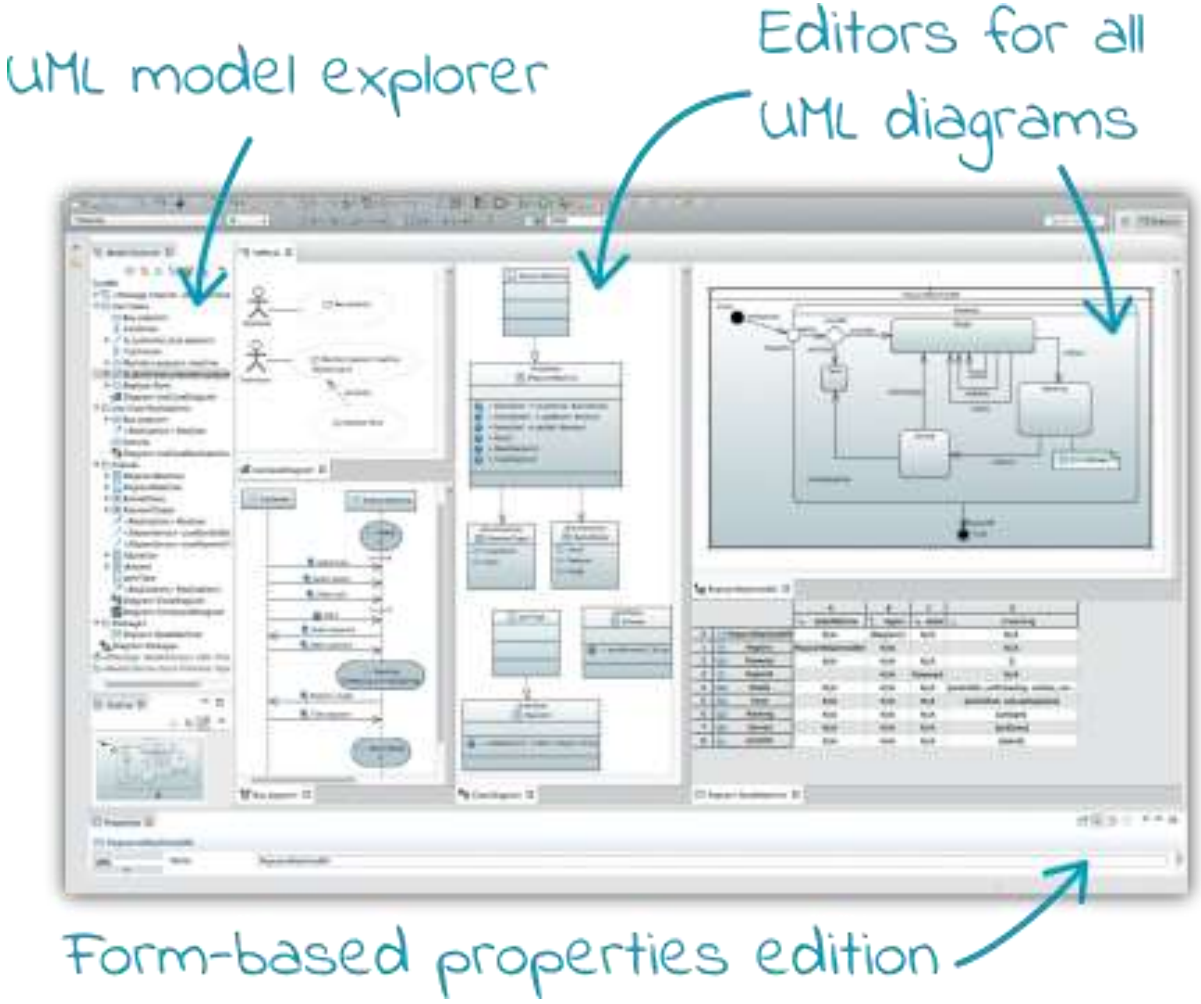


GDPR modelling in OpenCert: Reference Framework and Assurance Patterns

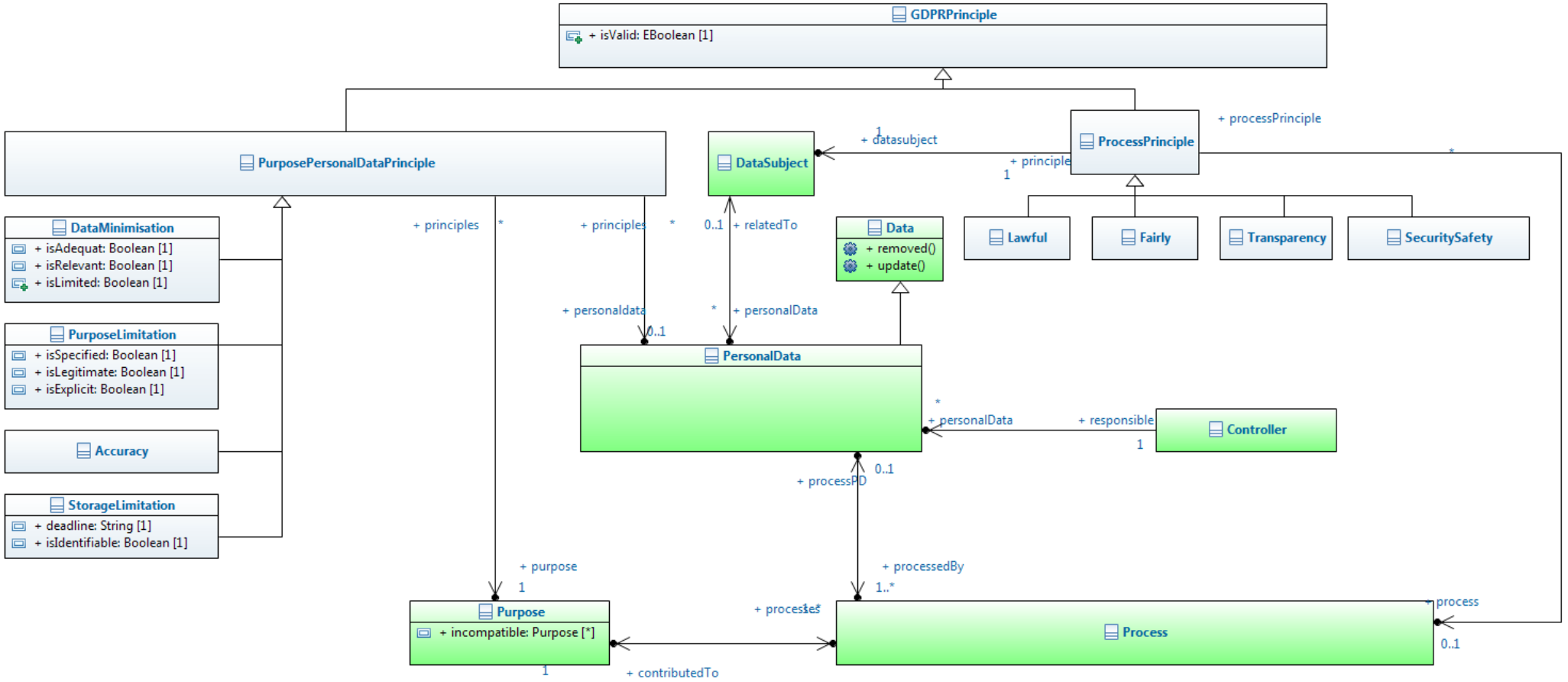




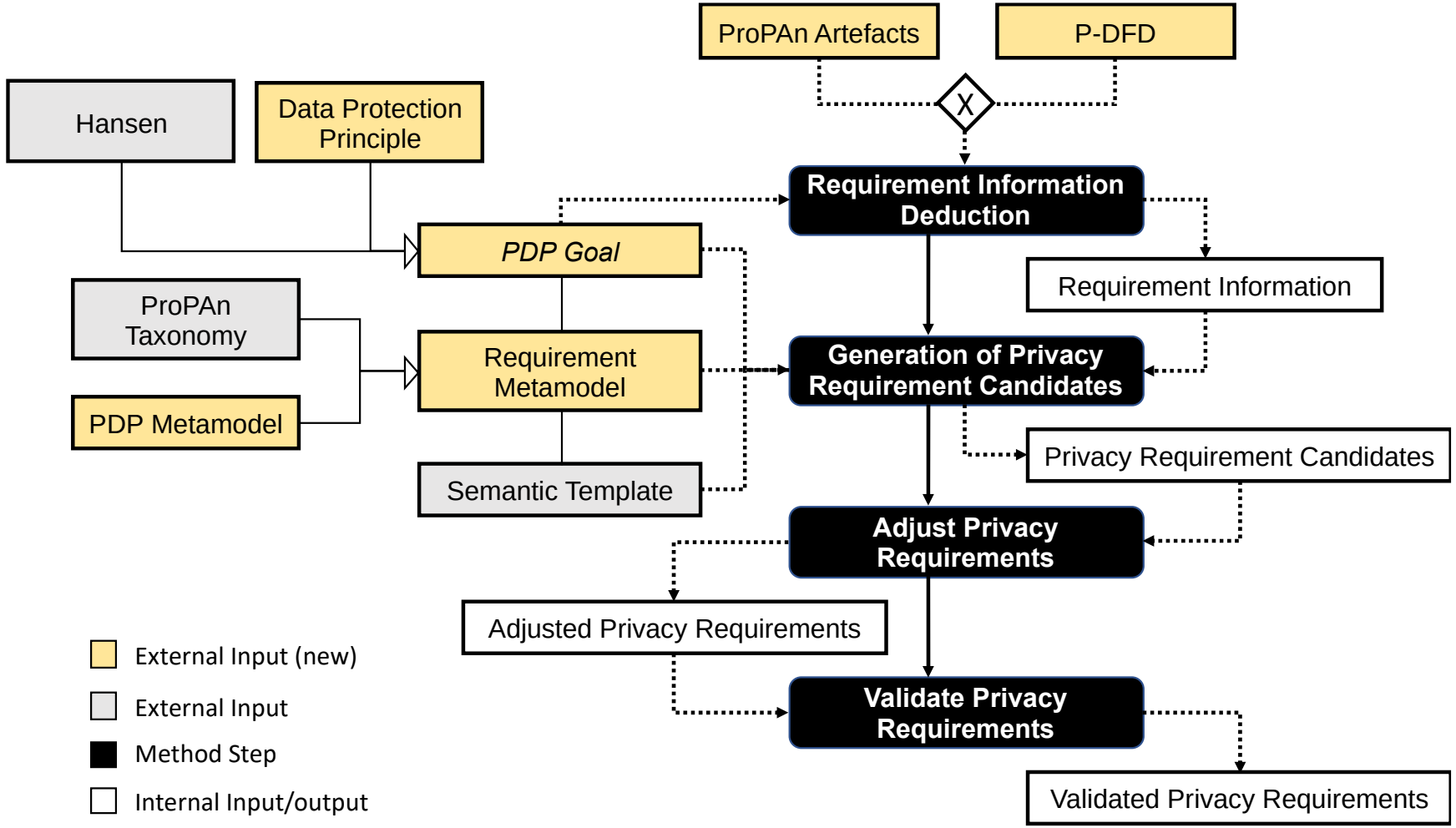
Papyrus overview



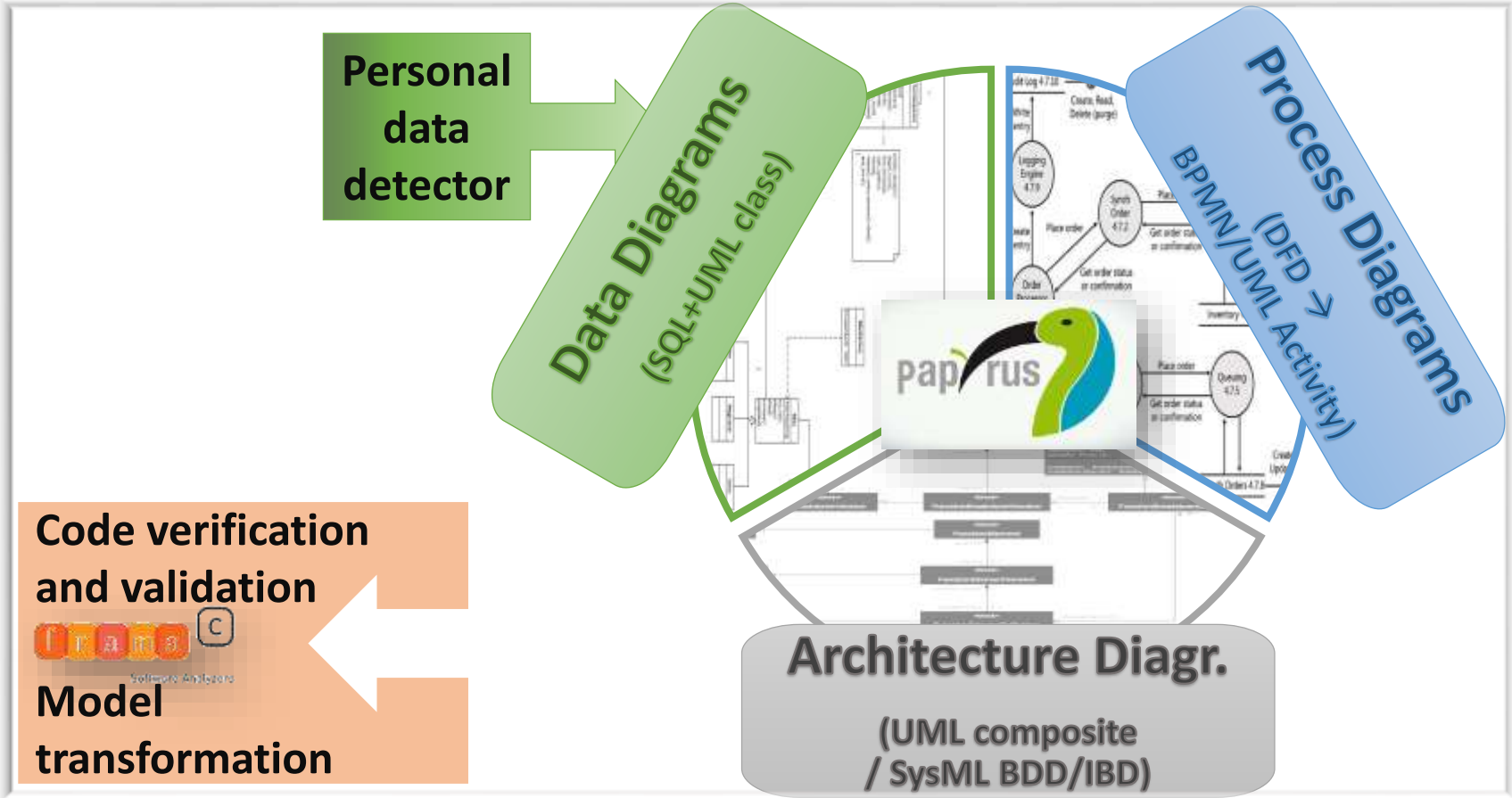
Privacy & data protection requirements metamodel (through Papyrus)

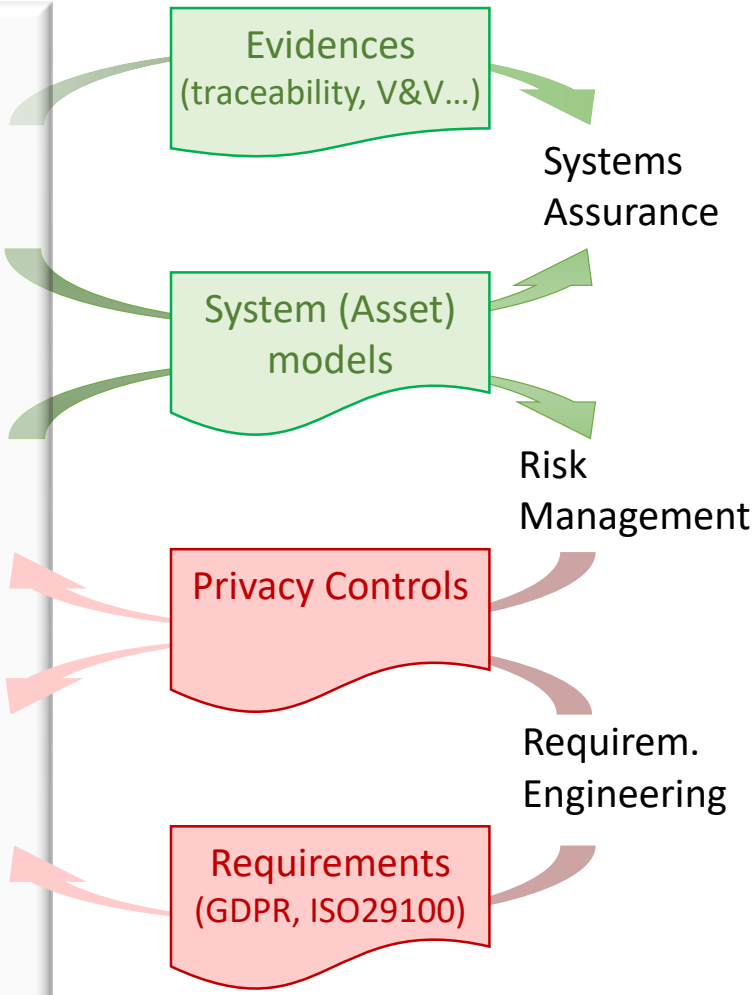


PDP4E Privacy & data protection requirements engin. method



Modelling-driven design for Privacy and Data Protection engineering (through Papyrus)





Privacy & data protection model-driven design. method

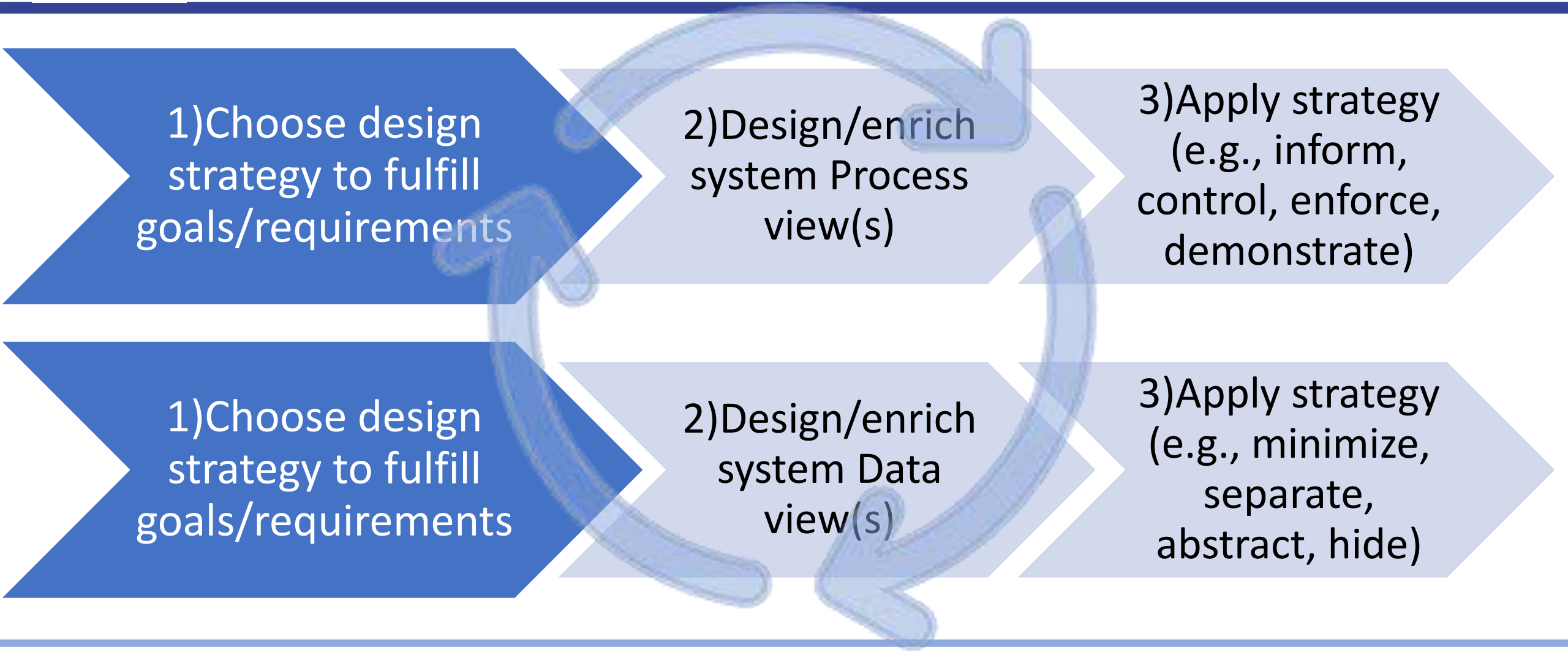


Image sources

- 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:
  - How GDPR Will Change The Way You Develop https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/ by Heather Burns, at Smashing Magazine.
  - 15 steps to developing GDPR-compliant apps https://techbeacon.com/security/15-steps-developing-gdpr-compliant-apps by Johanna Curiel, at TechBeacon.
  - 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 by Struu blog on Medium.
  - What Developers Need to Know About Europe's Data Privacy Rules https://spectrum.ieee.org/at-work/tech-careers/what-developers-need-to-know-about-europes-data-privacy-rules by Jeremy Hsu, at IEEE Spectrum
  - Your Guide to the GDPR https://spectrum.ieee.org/telecom/internet/your-guide-to-the-gdpr by Rosa María García Sanz, at IEEE Spectrum.
  - 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 by Bryan Soltis, at Hackernoon blog on Medium.
- Slides 3, 10 (images here cited under right of quotation or provided by PDP4E partners, unless otherwise specified):
  - Judge Gavel https://www.publicdomainpictures.net/en/view-image.php?image=164515&picture=judge-gavel by George Hodan, image in the public domain.
  - Privacy by Design 7 principles http://privacybydesign.ca/ (offline) by Ann Cavoukian
  - OneTrust privacy shield dashboard https://www.onetrust.com/es/products/ © OneTrust
  - 'Time to adopt' PETs poster © Enisa, use authorized under https://www.enisa.europa.eu/about-enisa/legal-notice
  - Papyrus captures from https://www.eclipse.org/papyrus/ , https://www.eclipse.org/papyrus/components/sysml/0.8.0/ , https://www.polarsys.org/list-of-projects © Eclipse Foundation, Inc.
  - OpenCert capture https://www.amass-ecsel.eu/content/opencert-base-tool-amass-management-assurance-and-compliance © Tecnalia, used under authorization.
- Slide 7: Figure cited from NOTARIO, Nicolás, et al. PRIPARE: integrating privacy best practices into a privacy engineering methodology. In *2015 IEEE Security and Privacy Workshops*. IEEE, 2015. p. 151-158.
- 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 by elisa_abuyah licensed under CC-BY--2.0 license https://creativecommons.org/licenses/by/2.0/
  - SysML IBD http://www.conceptdraw.com/solution-park/resource/images/solutions/software-sysml/Software-Development-SYSML-Block-Definition-Diagram.png by CS Odessa, licensed under the Creative Commons Attribution 4.0 International license.

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