Methods and Tools for GDPR Compliance through

PDP4E

Privacy and Data Protection 4 Engineering

Project Official Presentation

Coordinator: Trialog (Antonio Kung)

Scientific&Technical leader: UPM (Yod Samuel Martin)

H2020 Program

PDP4E

Outcome

- Mission & Consortium
- Objectives
- Context
  - Challenge of GDPR
  - What engineers get
  - What engineers need
- Contribution
  - Risk Management
  - Requirements Engineering
  - Model-driven Design
  - Assurance
  - Method Engineering
- Implementation
  - WorkPlan
  - Milestones
- Validation, demonstration and exploitation

PDP4E Mission & Consortium

- Mission: provide methods and software tools to
  - systematically apply data protection principles
  - And comply with the General Data Protection Regulation (GDPR)
- Partners
  - Trialog (FR)
  - UPM (ES)
  - Eclipse foundation (DE)
  - CEA (FR)
  - CA (ES)
  - Tecnalia (ES)
  - KU Leuven (BE)
  - U.Duisburg-Essen (DE)

PDP4E Objectives

- O1: Privacy by design and data protection in existing mainstream software and system engineering tools
  - risk management (MUSA DST)
  - requirements management (Papyrus 4 Req)
  - design and modelling (Papyrus)
  - assurance (OpenCert)
- O2: Privacy by design and data protection activities in existing mainstream software and system engineering methods
  - LINDDUN, PRIPARE, PROPAN, UML4PF
  - ISO 15288, OASIS PMRM, ISO 29134, ISO 27550

PDP4E Objectives

- O3: Knowledge repositories
  - operational data protection requirements
  - data protection risks, threats and solutions
  - privacy patterns
  - assurance reference frameworks
- O4: Fostering mainstream tools
  - Open source toolset EPL (Eclipse Public License)
  - Adaptability, flexibility and interoperability of PDP4E toolset
    - MDE approach
    - standard interchange formats

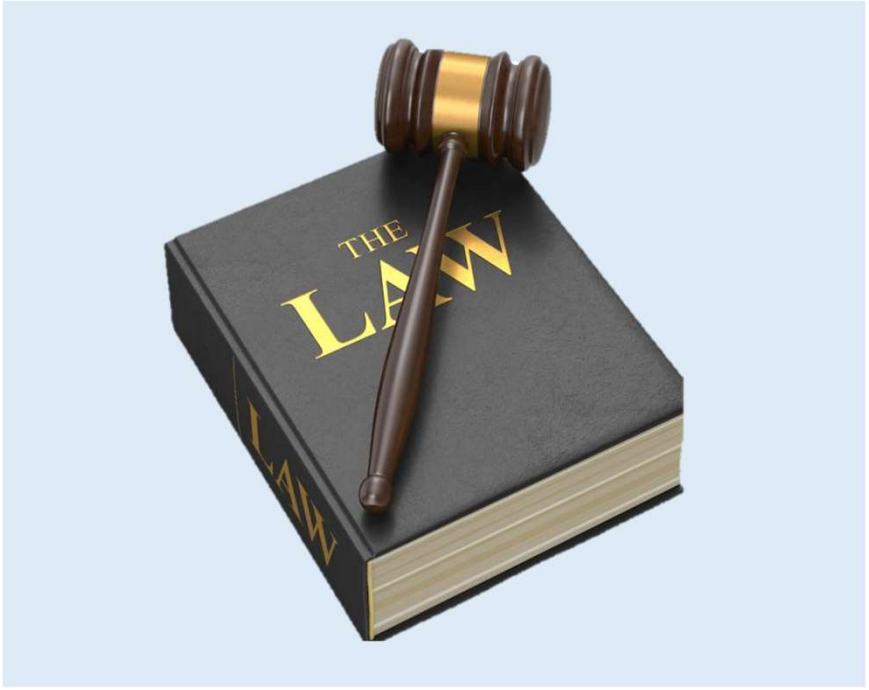
PDP4E Objectives

- O5: Increase privacy and data protection engineering practice
  - IPEN
  - Creation of an Alliance for Privacy and Data Protection Engineering
  - Standardisation
- O6: Two demonstration pilots
  - Fintech applications and services
  - Big data on smart grid

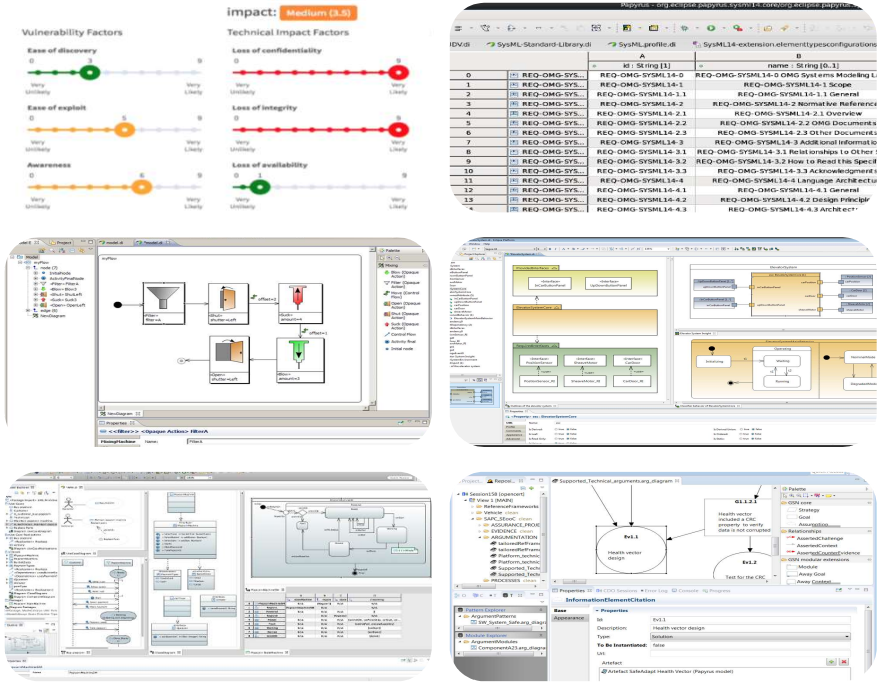
PDP4E

CONTEXT: GDPR Challenge

- What engineers get…



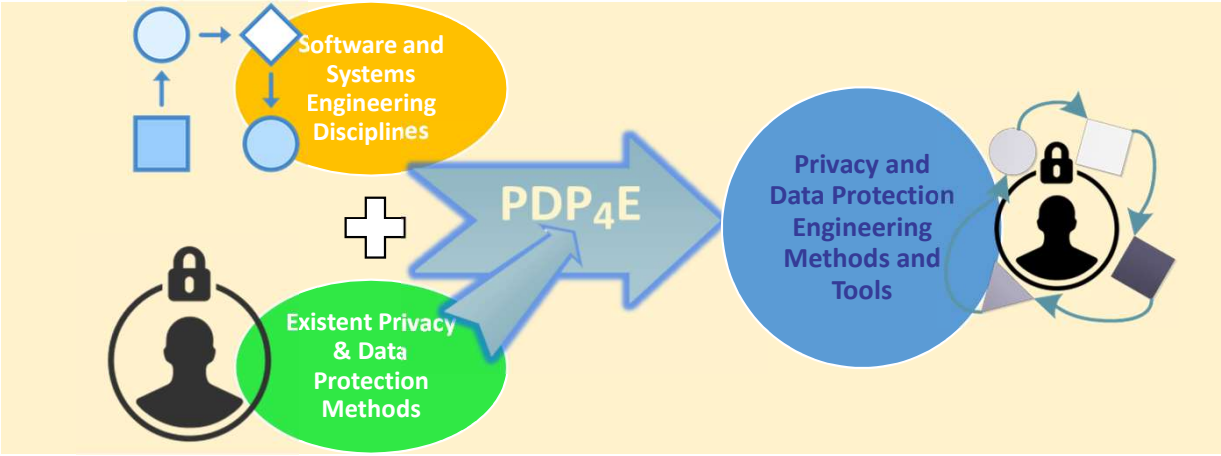
- What engineers want…



PDP4E

CONTEXT: What engineers need

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



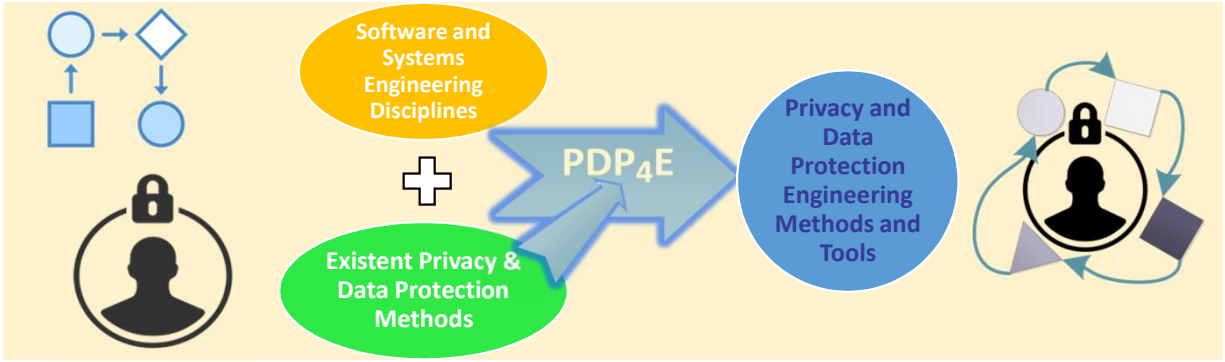
- Engineers are not privacy experts, yet they will face privacy issues (even if they may get expert advice)
- Privacy adoption entails for methods and tools integrated within the large heritage of software & systems engineering

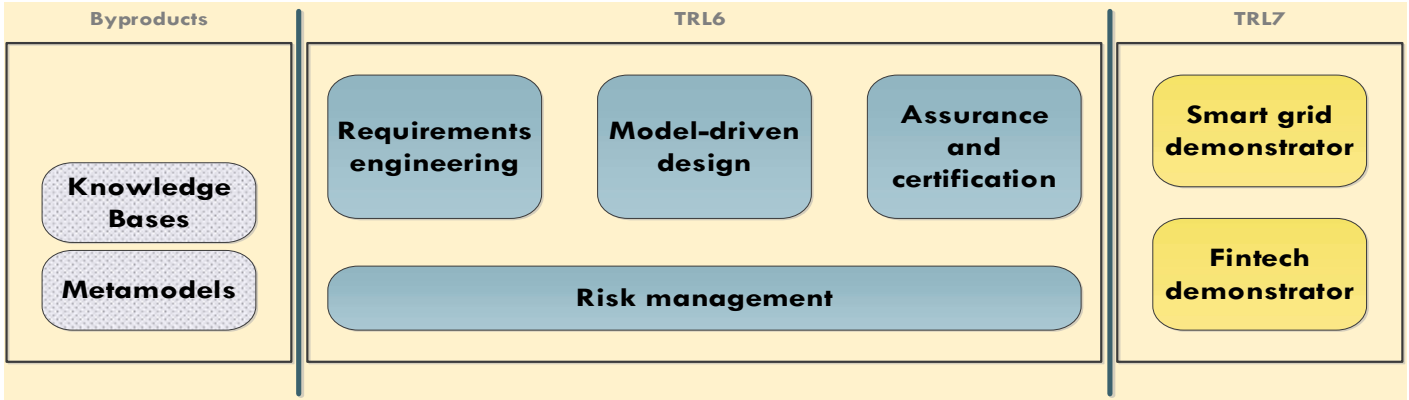
1. Seamlessly include privacy into software & system engineering tools
2. Integrate privacy activities into the SDLC stages
3. Provide a readily available body of knowledge with existent wisdom
4. Foster a community of privacy engineering

PDP4E

CONTEXT: What engineers need

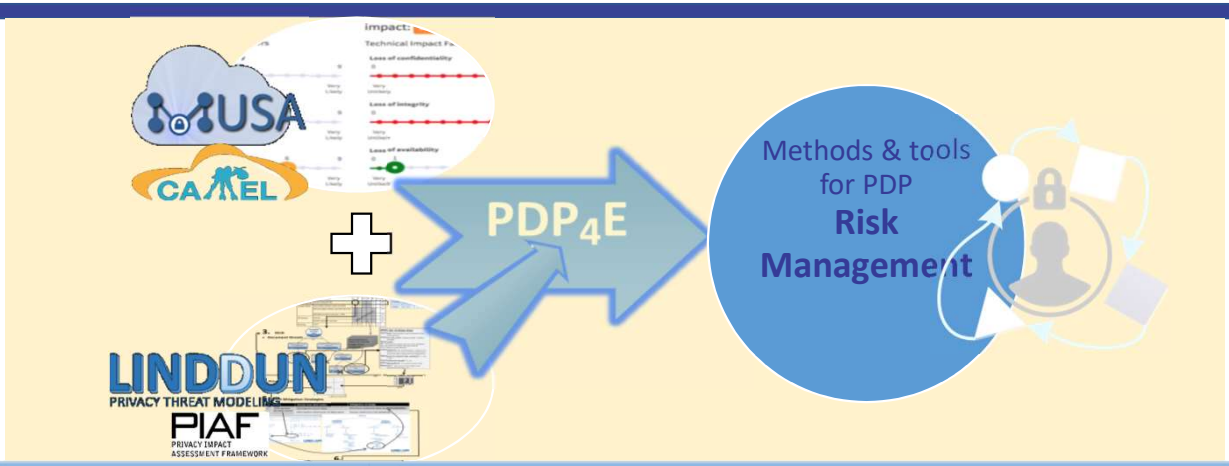
- Endow engineers with privacy and data protection tools aligned to their mindset





PDP4E

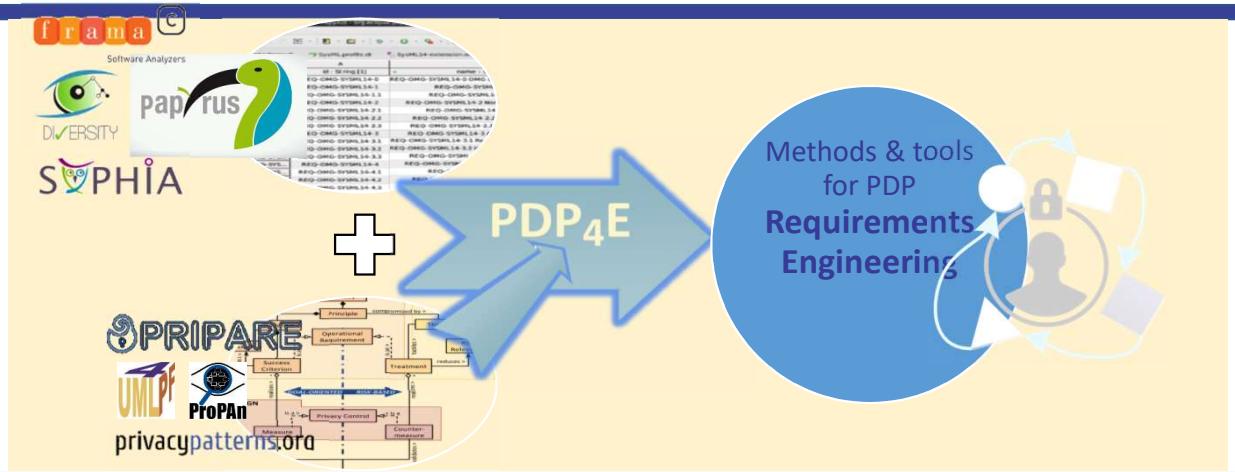
CONTRIBUTION: Risk Management



Identify, assess, evaluate and mitigate risks for the data subjects. Knowledge base of threats and countermeasures.	Data protection impact assessments (art. 35, besides WP29 guidelines on DPIA, rec. 84, 89-93) from an engineering perspective, including the determination of a need for a DPIA, the identification of threats, their likelihood and impact; the elicitation of mitigation countermeasures, etc.
Mapping between privacy and security risk assessments.	Security impact assessment (art. 32.2.)
Impact analysis for the business.	Right to compensation and liability (art. 82), conditions for administrative fines (art. 83).

CONTRIBUTION: from Requirements Engineering

PDP4E



Model-based methods and tools to specify regulatory constraints and privacy principles, and operationalize them into solution-oriented requirements (privacy controls).

Requirements management, analysis, traceability and validation.

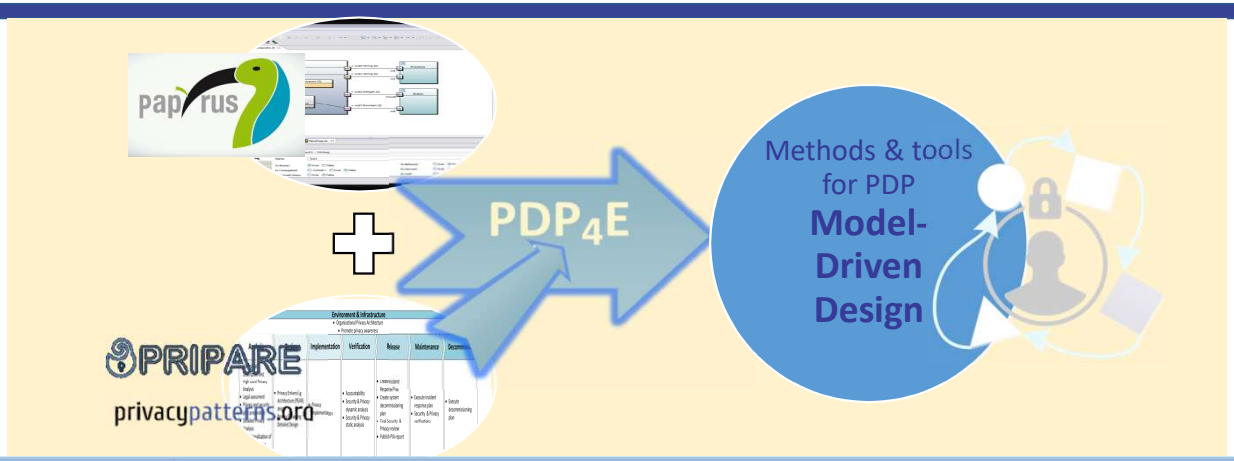
Knowledge base of data protection and privacy requirements and controls.

Principles relating to processing of personal data (Chapter 2), rights of the data subject (Chapter 3), obligations and responsibility of controllers and processors (Chapter 4, esp. art. 24 – 34) including technical and organisational measures (art. 24) and security (art. 32.1, especially par. d about assessment) [All these sections establish requirements with technical impact that need to be operationalized].

Requirements may also be derived from WP29/EDPB guidance (art. 70), codes of conduct (art. 40, 41), certifications (art. 42), binding corporate rules (art. 47) and derogations and exemptions anticipated by GDPR (art. 9.4, art. 49, Chapter 10, etc.)

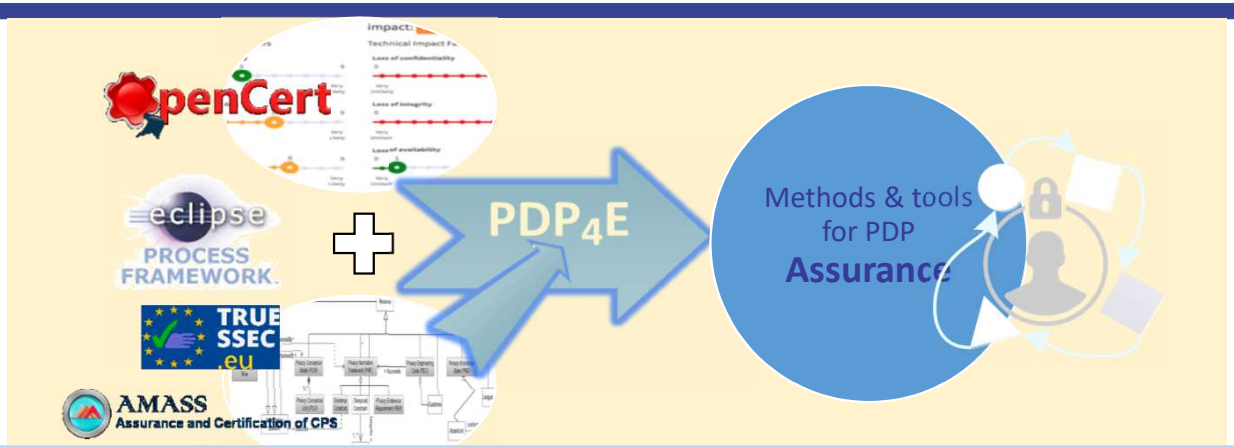
CONTRIBUTION: from Model-Driven Design

PDP4E



Analysis of annotated system models against the alignment to privacy and data protection principles, regulations and strategies; and transformation of those models when possible so as to comply with or apply such principles.	Principles of data minimisation (art. 5.1.c), pseudonymisation (art.4.5, art. 25), and confidentiality (art. 5.1.f), and controls for those aims (art. 25, art. 32). Minimisation in relation to the assessment of necessity and proportionality (art. 35.7.b). Obligations of processors (art. 28) and international transfers (art. 45, 46, 47, 49).

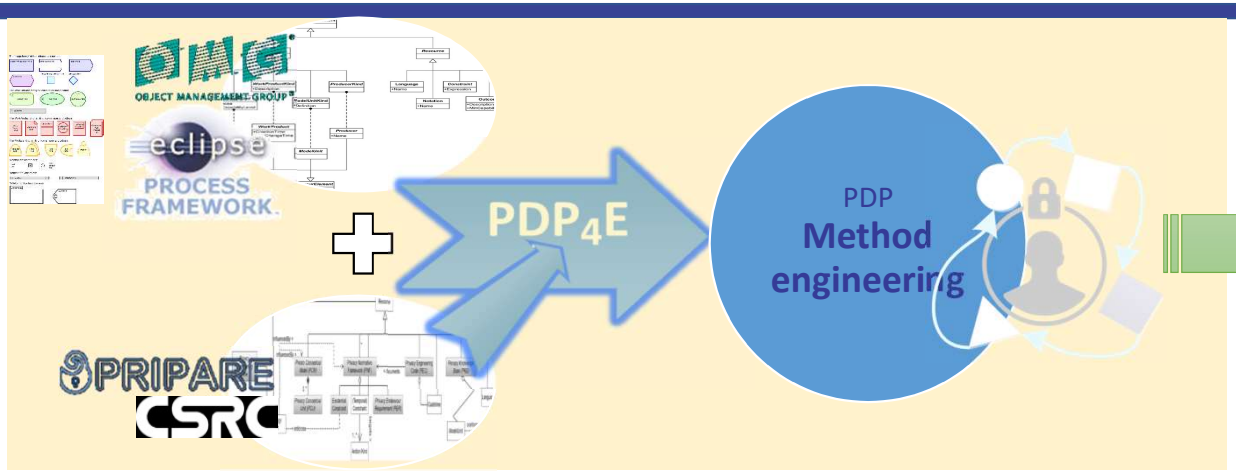
PDP4E CONTRIBUTION: from Assurance



Metamodels for data-protection regulatory framework and their interpretations and knowledge base (including model for GDPR and WP29/EDBP guidance)	Vocabulary to model GDPR general provisions (Chapter 1); models of processes and constraints established throughout GDPR; data protection policies (Art. 24.2). Interpretation in the form of WP29/EDPB guidance (art.70), and derogations and exemptions (art. 49, Ch. 10) Co-regulation methods expected by GDPR: codes of conduct (art. 40, 41), certification (art. 42), binding corporate rules (art. 47).

CONTRIBUTION: from Method Engineering

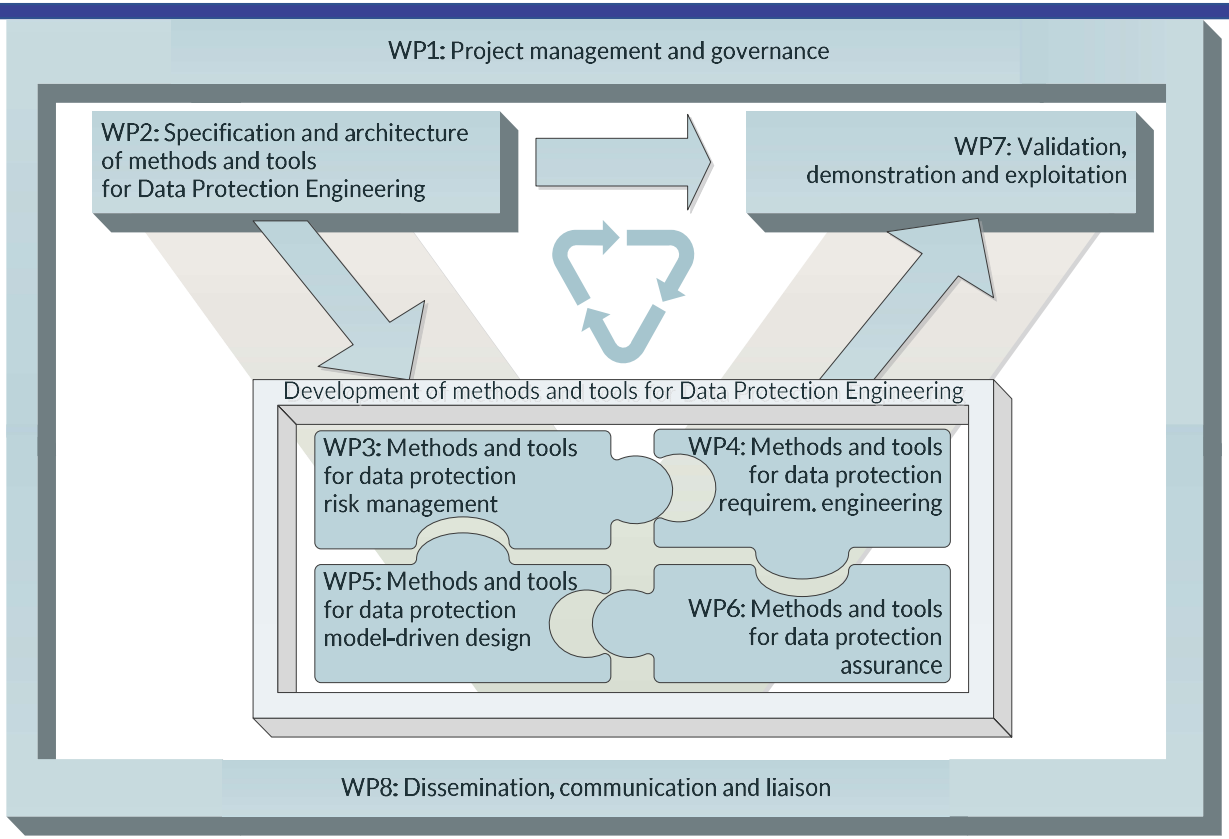
PDP4E



Privacy Method Engineering	Adaptability	Inherent toolset flexibility
• Putting it all together • Dependencies between one another • Methodologies and method fragments: work products, roles, tools, tasks, activities, processes • Activities: management, analysis, design, implementation, testing, deployment, operation, maintenance, and disposal	• Development methodologies or SDLC • Software engineering tools • Regulations (WP29/EDPB guidance, codes of conduct, derogations, non-EU…)	• Modularity and loose coupling • MDE and metamodelling • Evolving knowledge base • Flexible background tools • Open-source distribution • Flexible methodology

PDP4E

Implementation: WorkPlan

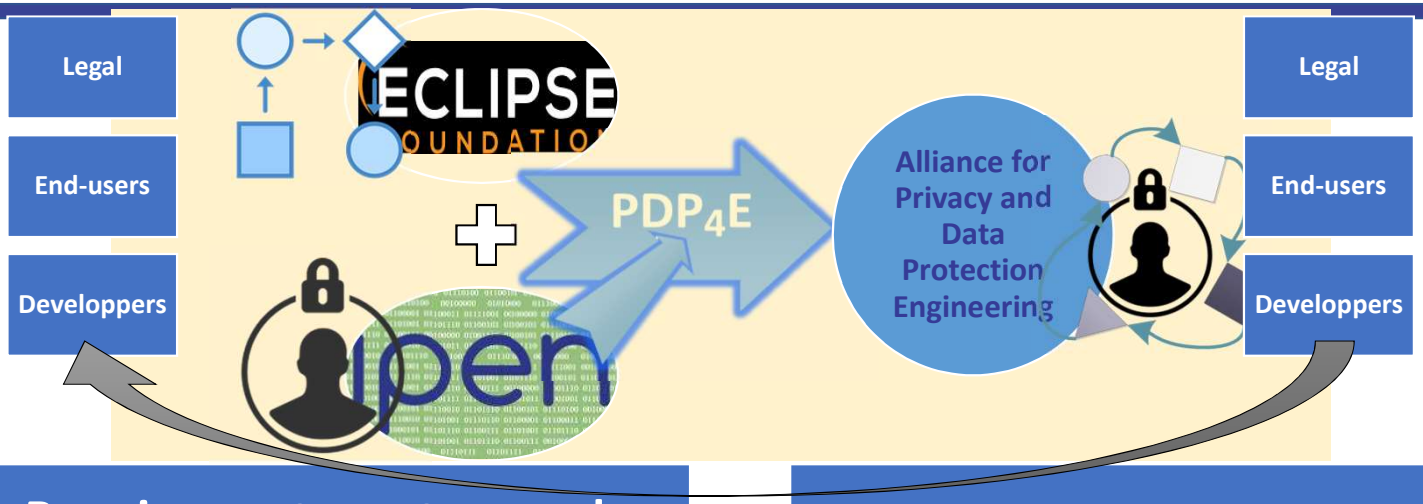


			MS1: Multi-stakeholder specification available					MS2: Architecture and design tools finalised					MS3: First release of tools and methods ready for use in the pilots						MS4: First user validation		MS5: Final release of tools and methods available for exploitation												MS6:Final validation & demonstration		
	Timeline	Leader	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
WP1	**Project management and governance**	**Trialog**																																	
T1.1	Strategic project steering	Trialog	D1.1																																
T1.2	Project administration	Trialog	D1.2										D1.3v1												D1.3v2									D1.3v3
T1.3	Quality management	UPM																																	
WP2	**Multi-stakeholder specification and architecture of methods and tools for data protection engineering**	**UPM**																																	
T2.1	Elicitation and analysis of market and user needs	CA			D2.1																														
T2.2	Legal and ethical analysis and constraints	KUL																																	
T2.3	Technical gap analysis and synthesis of user needs	Trialog					D2.2v1																												
T2.4	Architectural analysis and overall system requirements	UPM							D2.3v1																										
T2.5	Architechtural design, common interfaces, metamodel and formats	CEA										D2.4 v1																							
T2.6	Data Protection Engineering methodological framework	UPM																																	
T2.7	Architecture coordination, evolution and integration	UPM															D2.5v1				D2.2v2 D2.3v2 D2.4v2														D2.5v2
WP3	**Methods and tools for data protection risk management**	**CA**																																	
T3.1	Specification of risk management method elements	KUL											D3.2 v1								D3.2v2														
T3.2	Design and specification of the risk management tools for privacy and data protection impact assessment	CA									D3.1v1																								
T3.3	Development of the risk management engineering tools for stakeholders' evaluation	CA															D3.1v2 D3.3v1																		
T3.4	Consolidated implementation of the PDP risk management framework	CA																													D3.1v3 D3.3v2 D3.4			
WP4	**Methods and tools for data protection requirements engineering**	**CEA**																																	
T4.1	Specification of requirements engineering method elements	UDE											D4.2v1								D4.2v2														
T4.2	Design and specification of the requirements engineering tools for PDP	CEA									D4.1v1																								
T4.3	Development of the PDP requirements engineering tools for stakeholders' evaluation	CEA															D4.1v2 D4.3v1																		
T4.4	Consolidated Implementation of the PDP requirements engineering framework	CEA																													D4.1v3 D4.3v2 D4.4			
WP5	**Methods and tools for data protection model-driven design**	**CEA**																																	
T5.1	Specification of model-driven design method elements	UPM											D5.2v1								D5.2v2														
T5.2	Design and specification of the engineering tools for PDP modeling and conformity analysis	CEA									D5.1v1																								
T5.3	Development of the PDP model-driven engineering tools for stakeholders' evaluation	CEA															D5.1v2 D5.3v1																		
T5.4	Consolidated implementation of the PDP model-driven engineering framework	CEA																													D5.1v3 D5.3v2			
WP6	**Methods and tools for data protection assurance**	**TEC**																																	
T6.1	Specification of PDP assurance method elements	UPM											D6.2v1								D6.2v2														
T6.2	Design and specification of the PDP assurance tools for compliance and accountability	TEC									D6.1v1																								
T6.3	Development of the PDP assurance tools for stakeholders' evaluation	TEC															D6.1v2 D6.3v1																		
T6.4	Consolidated implementation of the PDP assurance tools	TEC																													D6.2v3 D6.3v2 D6.4v1			
WP7	**Validation, demonstration and exploitation**	**CA**																																	
T7.1	Validation and pilot for the smart grid market	CEA																	D7.3v1																D7.4 D7.5
T7.2	Validation and pilot for the fintech market	CA																	D7.3v1																D7.4 D7.5
T7.3	Validation by the community of users	ECL																	D7.3v1																D7.4 D7.5
T7.4	Legal validation and ethical impact assessment	KUL																	D7.3v1												D7.3v2				D7.4 D7.5
T7.5	Innovation and exploitation management	CA					D7.1v1						D7.1v2												D7.1v3										D7.1v4
T7.6	Open Source community and IPR management	ECL						D7.2					D7.1v2												D7.1v3										D7.1v4
T7.7	Standardization	Trialog																																	D7.1v4
WP8	**Dissemination, communication and liaison**	**UPM**																																	
T8.1	Scientific dissemination	UPM											D8.2v1												D8.2v2										D8.2v3
T8.2	Industrial dissemination	ECL											D8.2v1												D8.2v2										D8.2v3
T8.3	Communication and general dissemination	Trialog	D 8.1										D8.2v1												D8.2v2										D8.2v3
T8.4	Training	UDE																																	D8.3
	Consortium meetings (Workshop, Plenary, Review)		P	W			P				W/P					R		P		W/P		W		P		R				W/P				R

PDP4E Implementation: Milestones

No.	Name	Related WP(s)	Due date
MS1	Multi-stakeholder specification available	WP2	M5
MS2	Architecture and design of tools finalised	WP2-3-4-5-6	M10
MS3	First release of tools and methods ready for the pilots	WP3-4-5-6	M16
MS4	First user validation	WP7	M18
MS5	Final release of tools and methods	WP3-4-5-6	M30
MS6	Final validation and demonstration	WP7	M33

Validation, demonstration and exploitation



Requirements capture and validation

- Developers
- End-users
- Legal

Demonstration pilots

- Fintech pilot
- Smart-grid pilot

Methods and Tools for GDPR Compliance through

PDP4E

Privacy and Data Protection 4 Engineering

For more information, visit:
www.pdp4e-project.eu

Thanks for your attention

Questions?

Coordinator
Antonio Kung (Trialog)
Antonio.kung@trialog.com