# Models for Privacy

Yod Samuel Martín (Universidad Politécnica de Madrid)

Eclipse Models for Privacy Interest Group

November 23, 2023

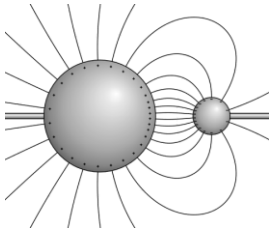
# Contents

- Frames the concept of ‘model’ and modelling languages
- Rationale for how to leverage models for privacy purposes.
- Defines a Domain-Specific Aspect modelling Language (DSAL) for privacy
  - i.e. a language of modelling concepts that can be attached to system models to describe its privacy-relevant properties.

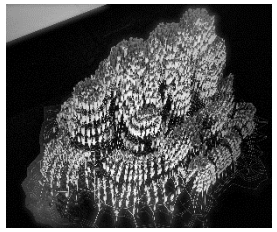
# What's (in) a model?

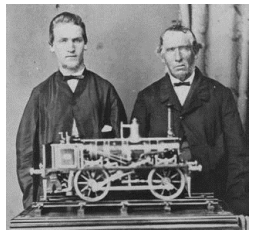
## Descriptive-ontological model

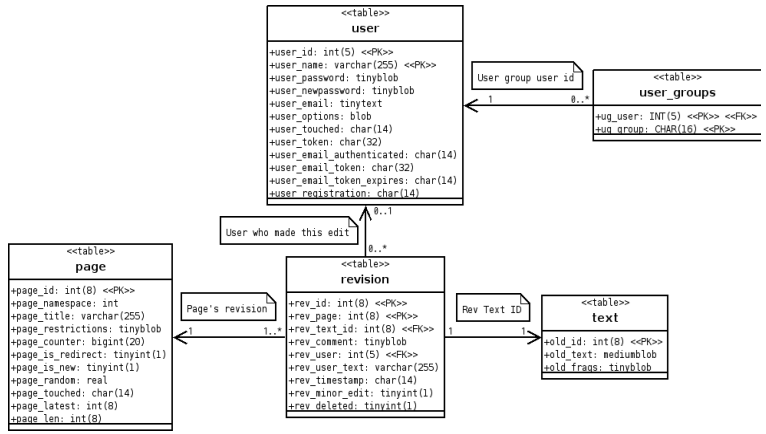
- (miniature) representation
- (mathematical) description
- (tangible) analogy



$$m\frac{\mathrm{d}^2\mathbf{r}(t)}{\mathrm{d}t^2} = -\nabla V[\mathbf{r}(t)]$$







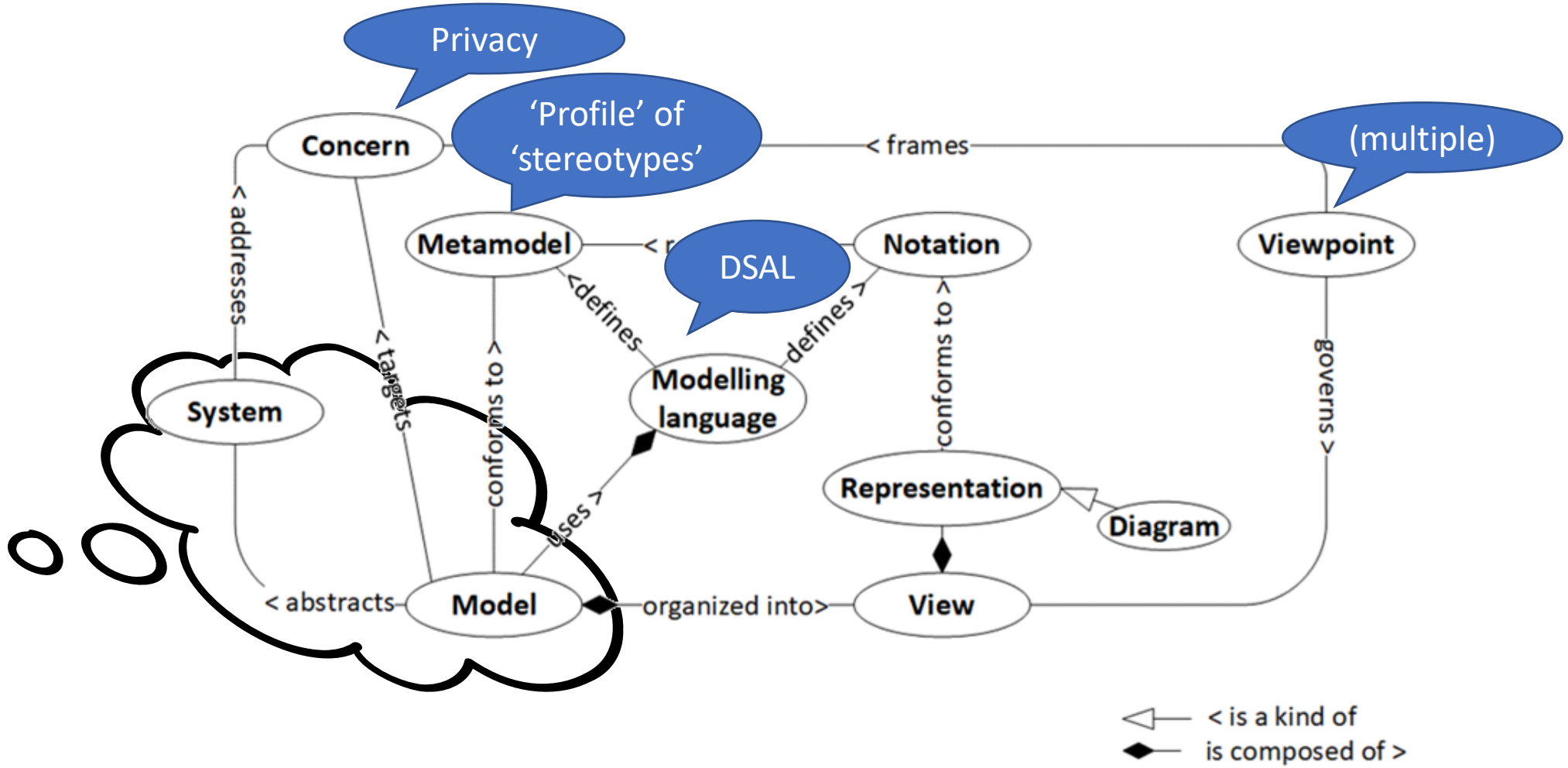

## Prescriptive-deontological model

- archetype for reproduction
- pattern to imitate
- example to emulate

➔ Patterns ➔

privacypatterns.org

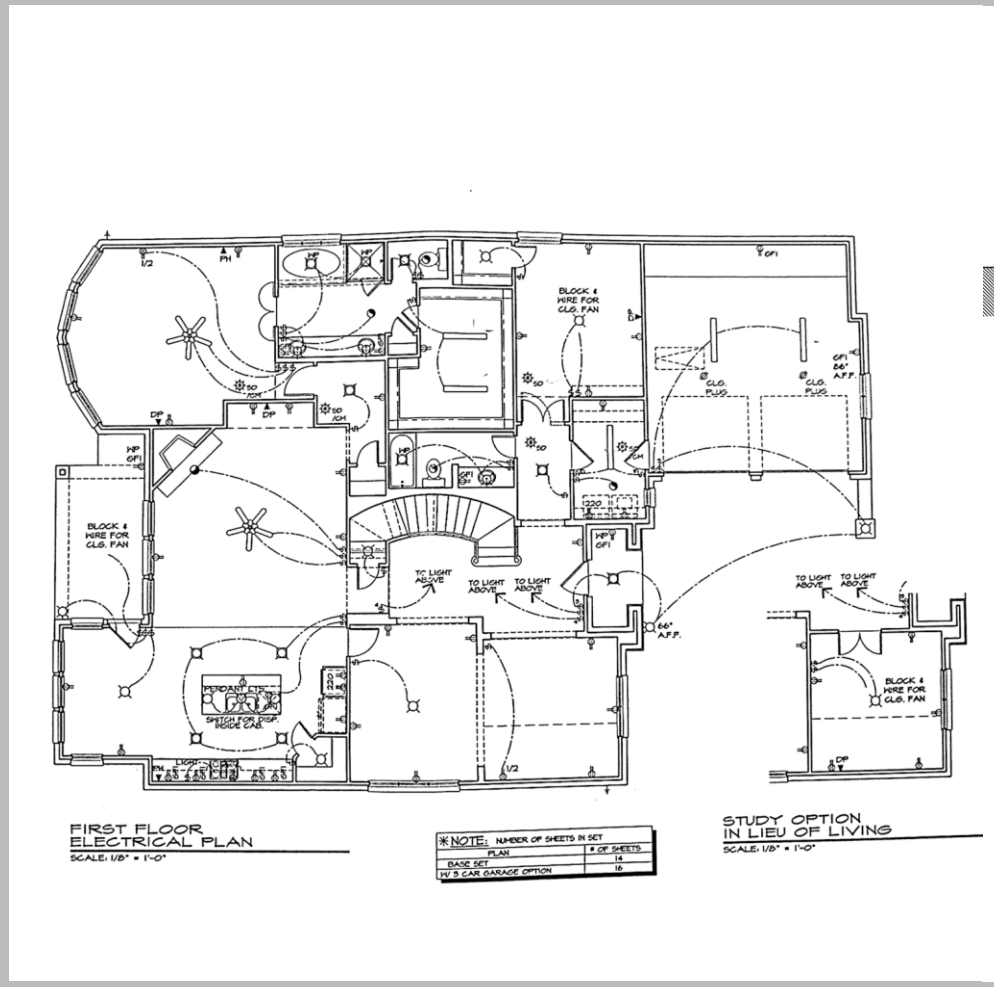
# Modelling for privacy

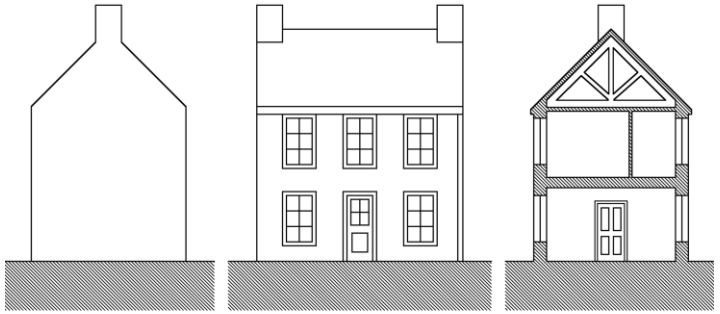


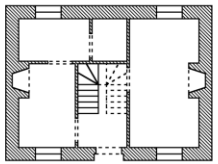
# Viewpoints (model of what?)

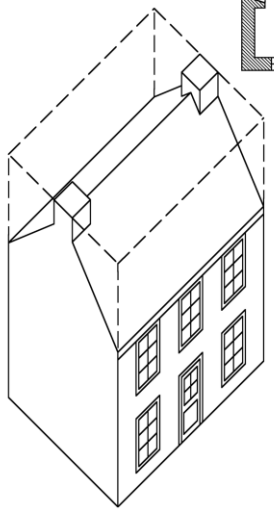
- System:
  - Data structures and relationships
  - Functions
  - Processes and data flows
  - Physical deployment
  - Timing
  - User interface
- System's context:
  - Requirements
  - Domain
  - Stakeholders and actors
  - Threats & risks
  - Regulations
- Development process:
  - Activities, artifacts, roles…
  - Assurance evidences & arguments

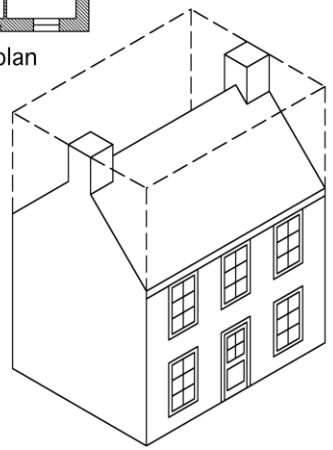
# Viewpoints (model of what?)

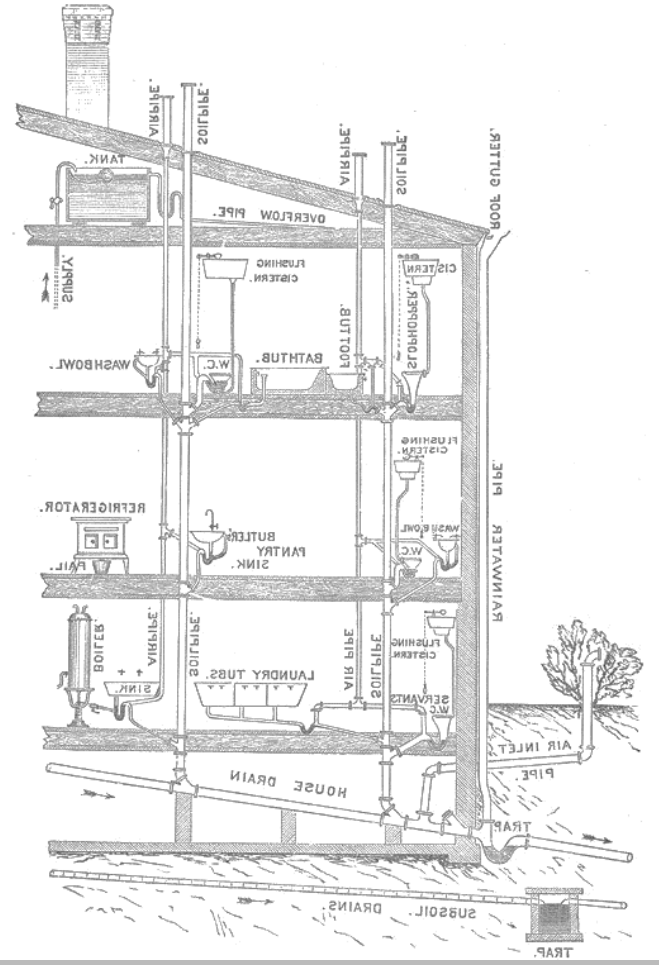


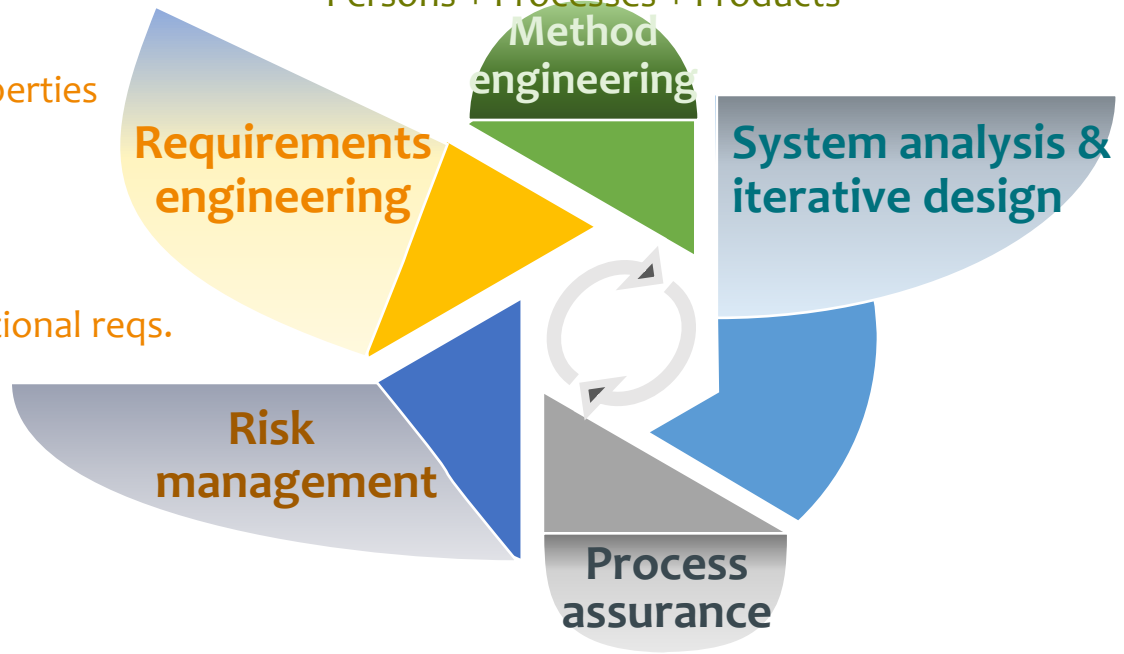



# Complementary modelling views and disciplines for privacy engineering

Dev. Process. Model:
Persons + Processes + Products




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?

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

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?

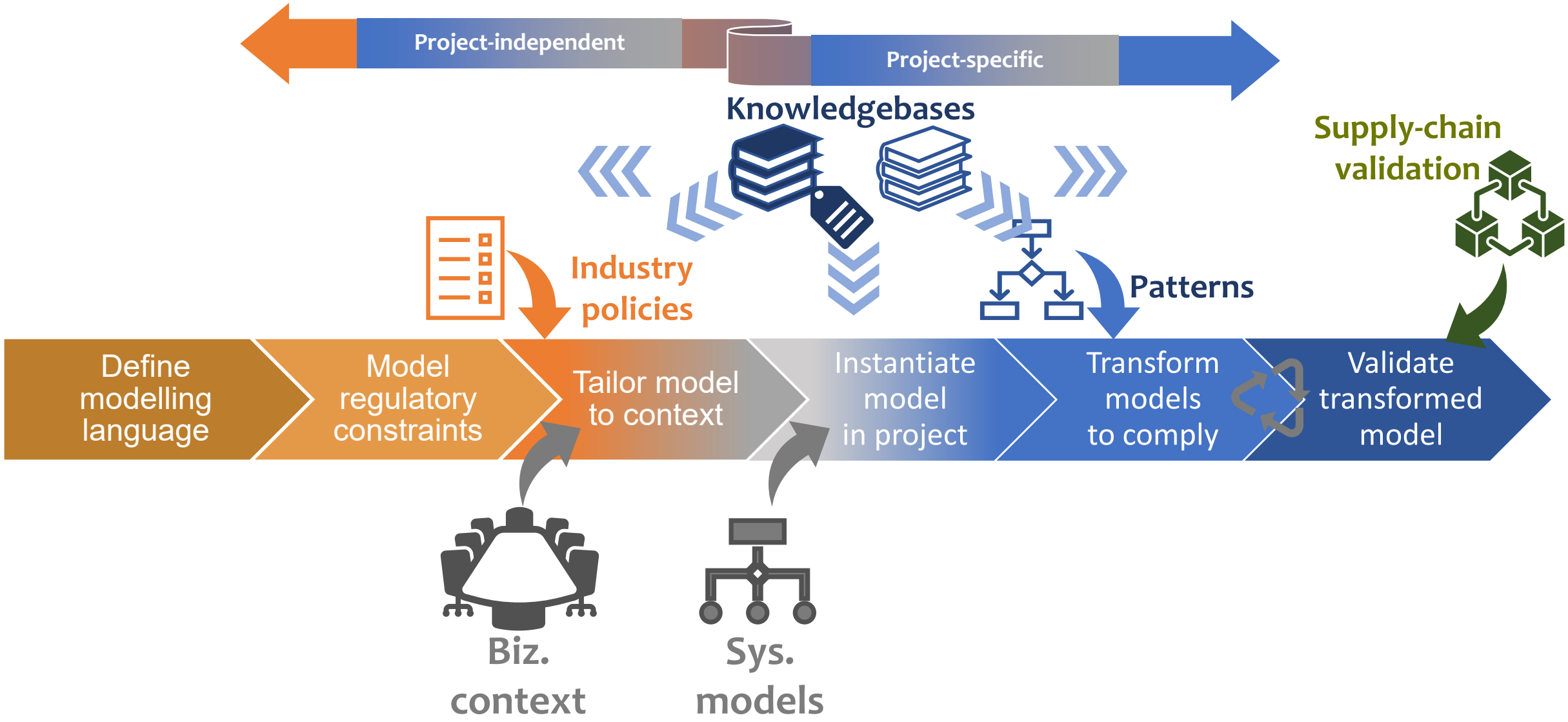
# Domain-specific privacy aspect modelling language

| Questions addressed | Stereotype |
|---|---|
| Which data is personal? | **«Personal Data»** |
| How sensitive it is? | |
| Where did it come from?<br>Why can it be collected and processsed? | |
| How do I know it is personal? | |
| Who is this data about? | **«Data subject»** |
| Who is authorized to access that data?<br>How do they know that they are authorized? | **«Usage policy»** |
| Which processes deal with personal data? Which processing operations it is being subject to?<br>For what purpose it is being used? | **«Data Processing Operation»** |
| How does data travel through processes? Which data goes from one process to another? | **«Data Flow»** |
| Who sends to and receives data from the system? | **«External entity»** |
| Where and how long is data stored? | **«Data Storage »** |
| To which data subject rights it applies? | **«Right supporting»** |
| Where is data processed (and collected, etc.)? | **«Processing node»** |
| Where does data go through? | **«Communications link»** |
| Who processes data?<br>Under which jurisdiction? | **«Realm»** |
| How is data protected? | **Common attributes** |

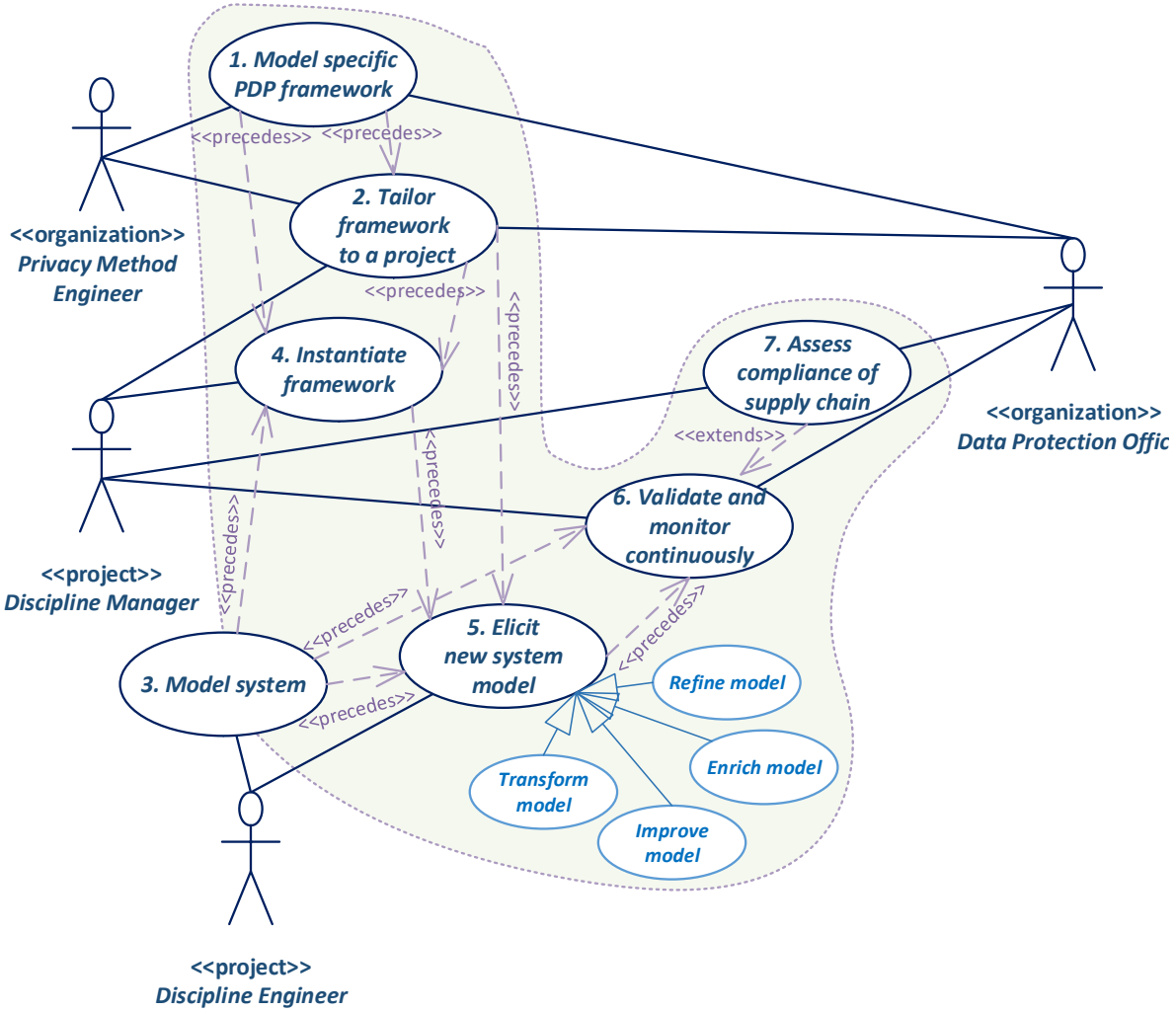
# Domain-specific privacy aspect modelling language

| Modelling viewpoint | Questions addressed | Contents |
|---|---|---|
| **Requirements model** | What features shall the system implement? Why? | - Privacy requirement templates / frames<br>- Source<br>- Ref. to functional requirements and system elements |
| **Risk model** | What do we need to protect?<br>What from?<br>How likely and damaging it may be? | Assets<br>Threats<br>Risk factors |
| | How do we (and others) protect them? | Controls |
| **Assurance model** | What shall I comply with?<br>How can I assure that I am compliant? | Reference framework<br>Evidences<br>Argumentations |
| **Methodology model** | How am I developing a privacy-compliant system?<br>What resources do I have? | Development processes, people and products<br>Development resources including privacy normative framework, knowledgebases, etc. |

# Model-based privacy engineering lifecycle?



# Alignment to 24641 MBSSE




ISO/IEC/IEEE CD 24641:2020(E)