

Regulations are specified according to the legal knowledge. For this reason, it is useful to use a conceptual model to process text of regulations in a structured way. In this exercise we would like to introduce you to a model-based method for analysis of regulation and specification of requirements and systems in compliance with GDPR.

This exercise is composed of four parts:

- basic introduction into concepts and definitions for legal text annotation;
- checking examples of annotations and resulting models;
- annotation of text and extension of models with the identified concepts;
- evaluation of the method (after a joint discussion at the end of the workshop).

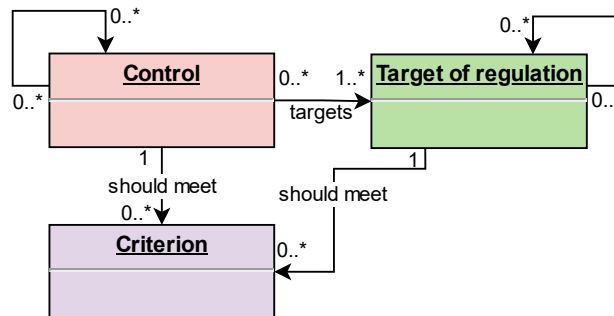
1 Model overview: concepts, their relationships and levels of abstraction

Target of regulations - existing components of software systems, organizational processes which are addressed in regulations

Compliance control - new or existing software components, organizational processes introduced to address the targets of regulation.

Criterion - properties of compliance controls AND/OR targets of regulations which qualify then as acceptable from the legal perspective.

The following class diagram shows the relationships between the concepts:



Herewith, possible relationships between the instances of concepts are as follows:

1. relationships between different instances of “target of regulation”;
2. relationship between “target of regulation” and “criterion”;
3. relationships between “control” and “target of regulation”;
4. relationships between “control” and “criterion”;
5. relationships between different instances of “control”.

These concepts are allocated across two levels of abstraction:

Requirements specification – including abstract concepts not specific to particular system-level specification and demanding additional interpretation.

System specification – including concepts directly related to system and not requiring additional interpretation.

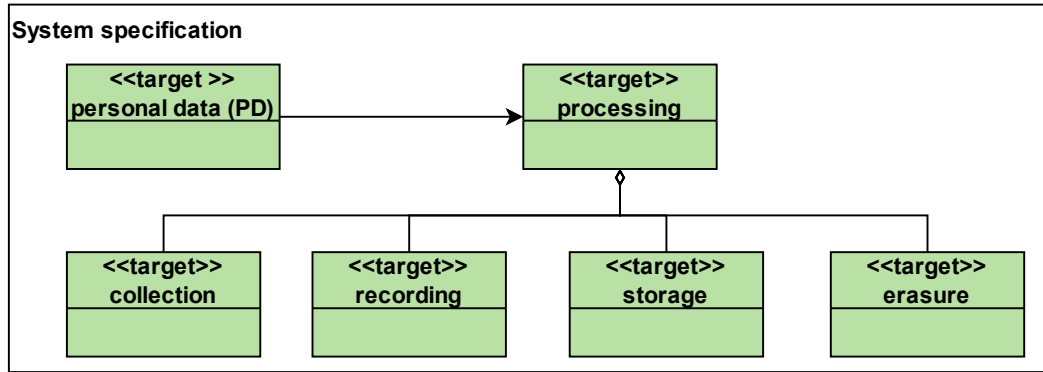
2 Examples of annotation of the concepts and models resulting from their analysis.

2.1 Example 1

Article 4

(2) **processing** means any operation or set of operations which is performed on **personal data [..]**, whether or not by automated means, such as **collection**, **recording [..]** **storage**, [..] **erasure** or **destruction**.

Resulting model:



2.2 Example 2

Article 6

1. **Processing** shall be **lawful** only if and to the extent that at least one of the following applies: (a) the data subject has **given consent** to the **processing** of his or her personal data **for one or more specific purposes**.

Resulting model:

