

Master Thesis: An Extension of Hybrid Wiki Meta-Model for Management of Personal Data

Ahmet Tanakol, 30.11.2018, Kick-Off Presentation, Munich

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
www.matthes.in.tum.de

1. Motivation

- GDPR
- Requirements for an Information System
- Hybrid Wikis

2. Research Approach

3. Use Cases

4. Current Progress

5. Timeline

GDPR: General Data Protection Regulation



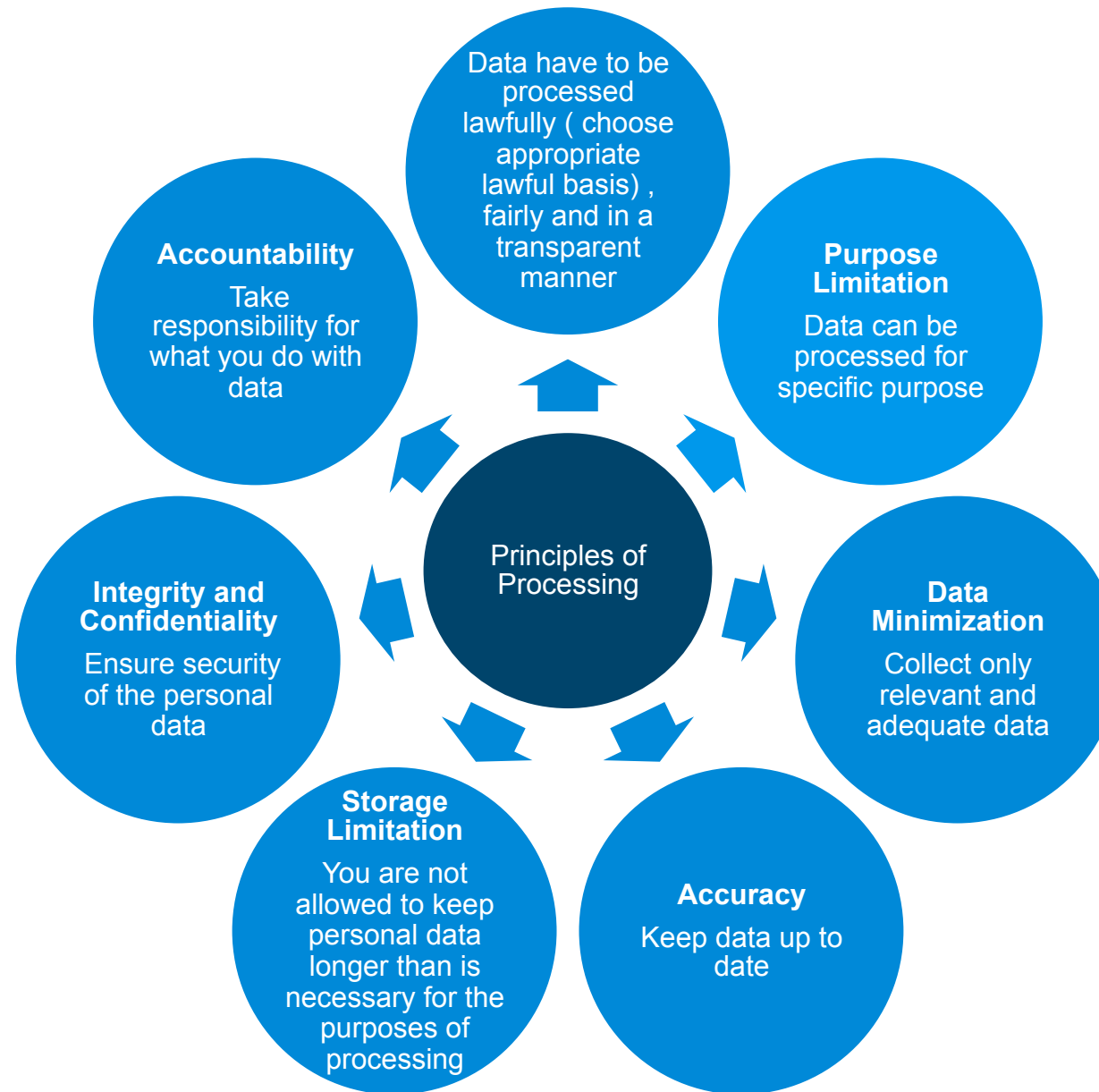
- ➔ Enforce privacy and protection over data for all individuals within the EU
- ➔ Allow individuals to have control over their personal data

What is personal data?

Article 4: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person [1];

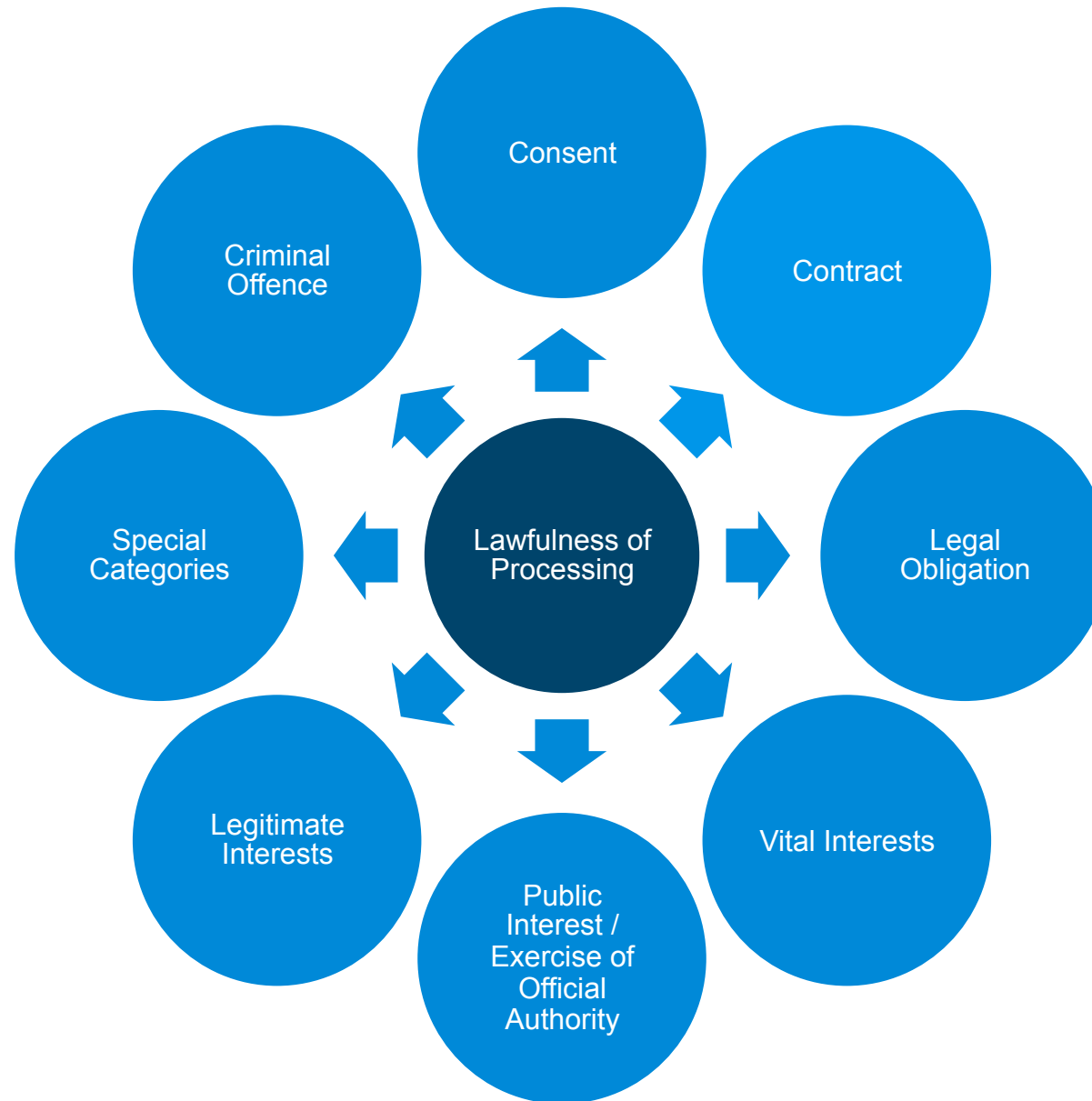
Motivation

GDPR – Article 5



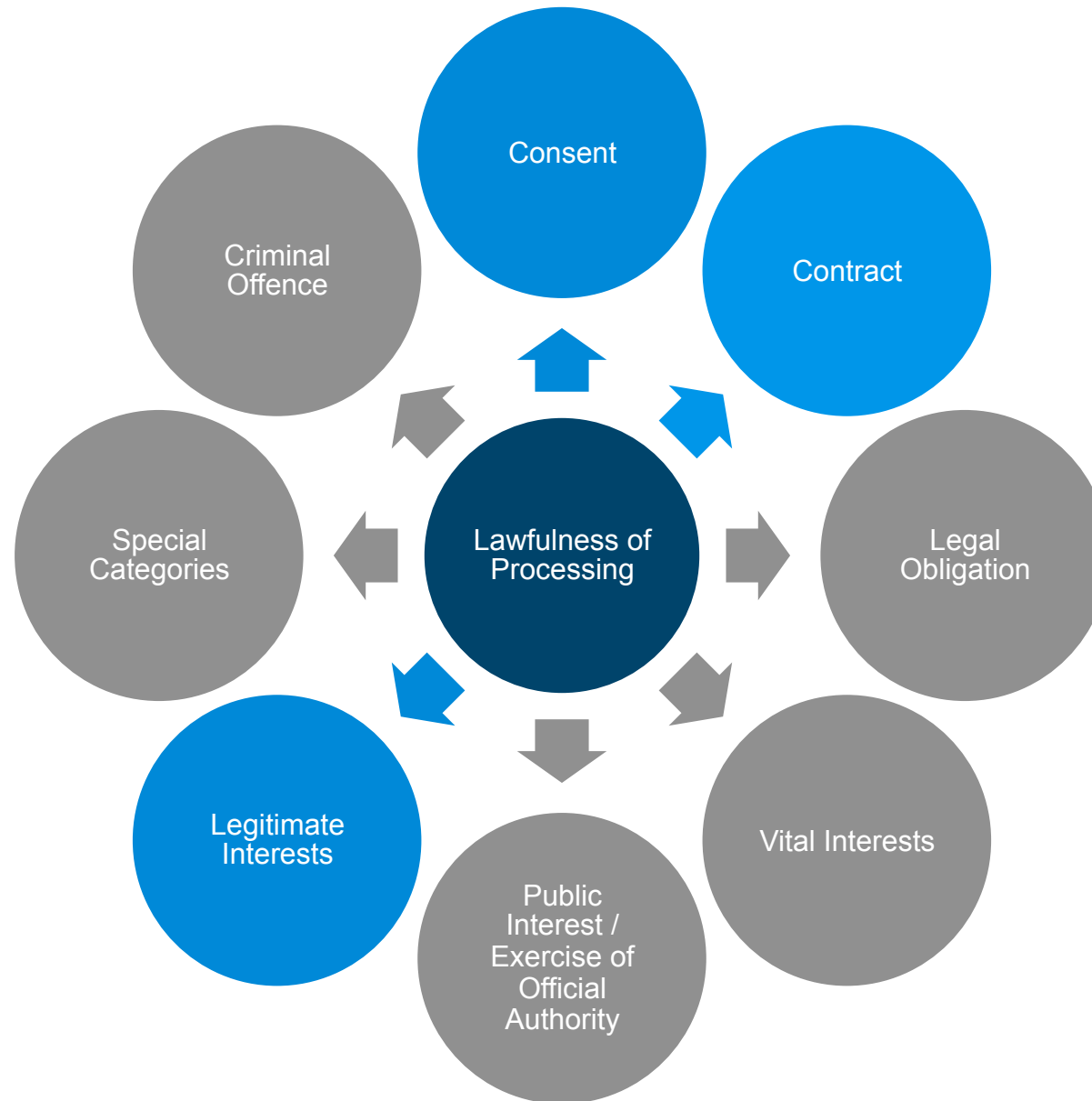
Motivation

GDPR – Article 6



Motivation

GDPR – Article 6



1. Motivation

- GDPR
- Requirements for an Information System
- Hybrid Wikis

2. Research Approach

3. Use Cases

4. Current Progress

5. Timeline

Requirements for an Information System

Principles	System Requirements
Lawfulness, fairness and transparency	• Store lawful bases (consent, contract, legitimate interest etc..) for processing activities • Provide prominent description about usage of personal data
Purpose Limitation	• Store purpose of each processing activity which is used to collect personal data
Data Minimization	• Store personal data only for specified purposes
Accuracy	• Data have to be modifiable
Storage Limitation	• Data have to be removable • Store retention period for data storage • Store conflicting legislation (i.e. to identify which personal data have to be stored for a long period of time)
Integrity and Confidentiality	• Limit access to personal data • Provide access control mechanism
Accountability	• Store records of processing activities • Store third parties that personal data are shared with • Keep track of changes of personal data (who did what, when) • Store information of person who is responsible for data processing activities

1. Motivation

- GDPR
- Requirements for an Information System
- Hybrid Wikis

2. Research Approach

3. Use Cases

4. Current Progress

5. Timeline

Hybrid Wiki system allows non-expert users to fill data in particular fields of a form or table without knowing any special knowledge about the modeling concepts in order to create structured information for unstructured contents. Semantic annotations can be created and added dynamically by users and it is possible to query structured part via user interfaces [3]. Hybrid Wiki system can be also used as model-based data repository [4].

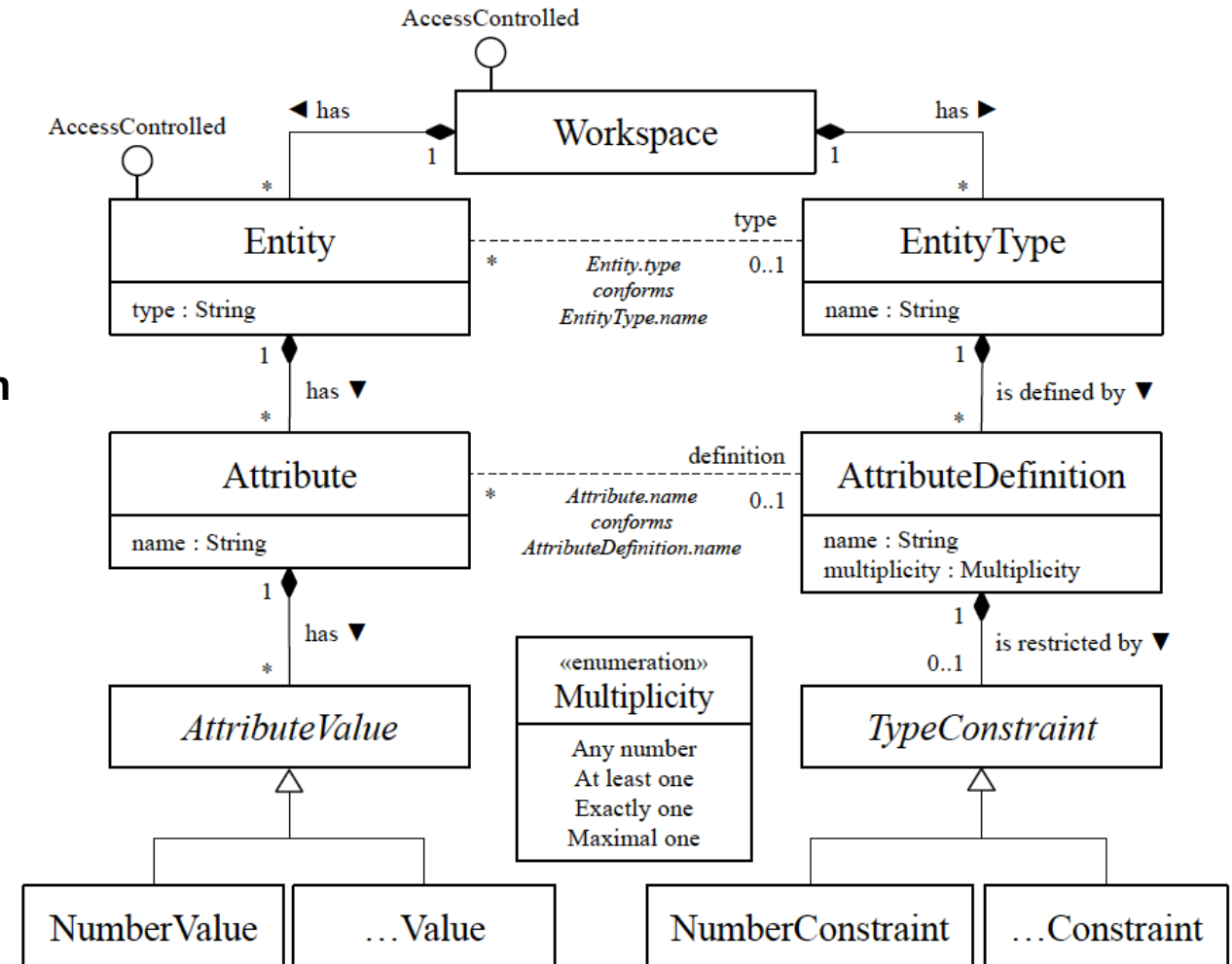


Figure 1: The updated Hybrid Wiki meta-model by Reschenhofer et al. [4]

How well does SocioCortex (Implementation of Hybrid Wiki Meta-Model) fit to the requirements

SocioCortex	Requirements	
Offer data management	Data can be stored, modified, deleted and accessed at any time.	✓
Allow to define new data models (connecting data to models via types with a set of attributes)	- Manage GDPR related data models in a structured way - Access and query to GDPR related information in a fast and easy way (i.e. incoming references of an instance) - Store various processing activities and related information about these activities - Data models of GDPR related applications can be defined	✓
Store unstructured content	Legal texts can be stored as wikis (i.e. description about usage of personal data)	✓
Define attributes to entity types (a predefined set of fields)	For every personal data object, it is possible to define necessary attributes such as data collection date or retention period.	✓
Access Control	- Limit access to personal data - Set read/write permissions for different kind of users	✓
Version History	Keep track of changes in data	✓

Motivation

Hybrid Wikis – GDPR Compliant Hybrid Wikis

Hybrid Wikis do not provide interface for addressing GDPR information requirements

There is a need for defining rules which can be used to evaluate some conditions and apply an effect, once the condition is met (i.e. add default attributes if user enables GDPR fields)

Research Goal:

The goal of this research is to extend Hybrid Wikis in a way that data models become readily conformant to GDPR processing principles

1. Motivation

- GDPR
- Requirements for an Information System
- Hybrid Wikis

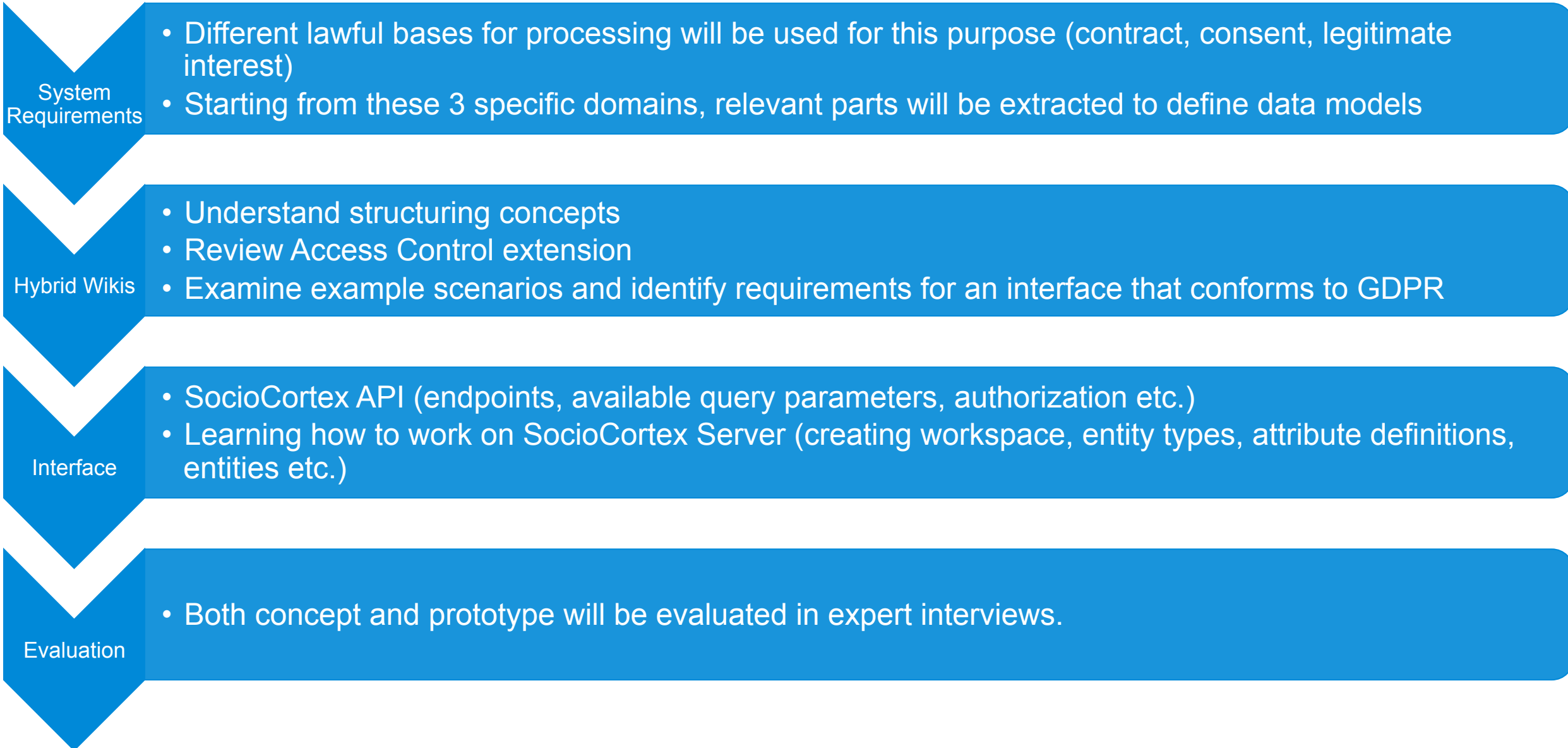
2. Research Approach

3. Use Cases

4. Current Progress

5. Timeline

Research Approach



1. Motivation

- GDPR
- Requirements for an Information System
- Hybrid Wikis

2. Research Approach

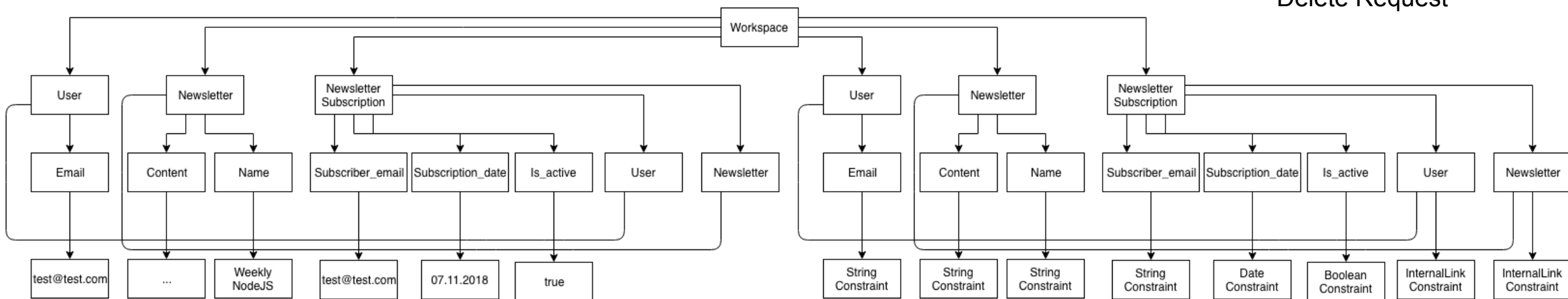
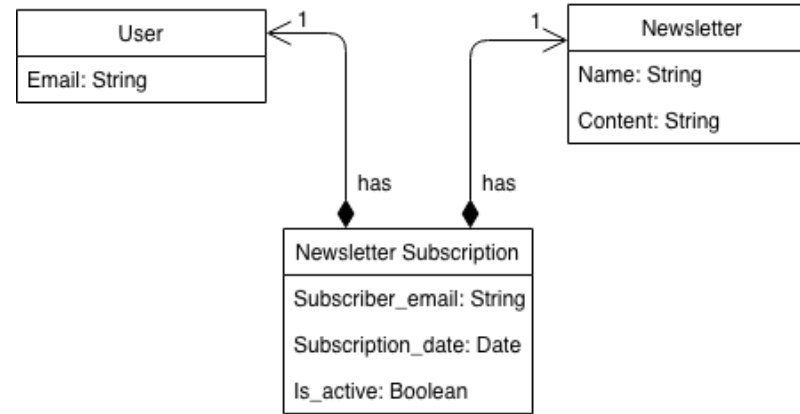
3. Use Cases

4. Current Progress

5. Timeline

Use Cases

Example 1 Consent – Newsletter Subscription



Requirements for GDPR compliance

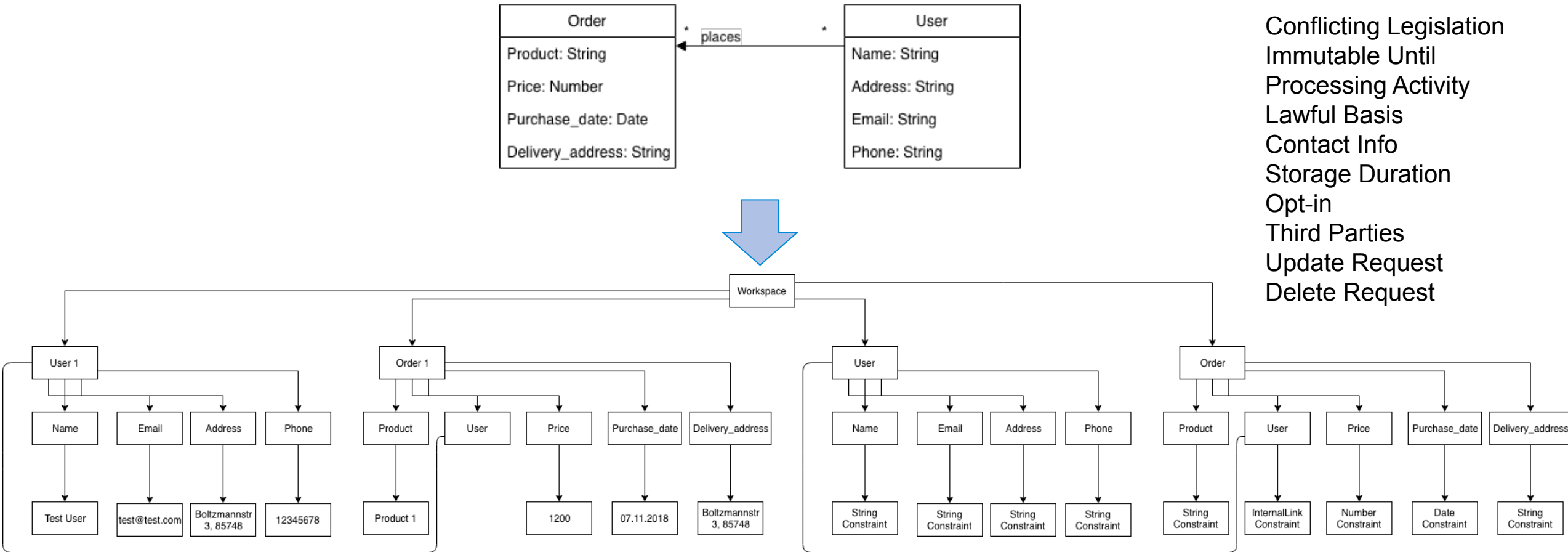
Conflicting Legislation
Immutable Until
Processing Activity
Lawful Basis
Contact Info
Storage Duration
Opt-in
Third Parties
Update Request
Delete Request

Use Cases

Example 2 Contract – Placing Order

Requirements for GDPR compliance

Conflicting Legislation
Immutable Until
Processing Activity
Lawful Basis
Contact Info
Storage Duration
Opt-in
Third Parties
Update Request
Delete Request

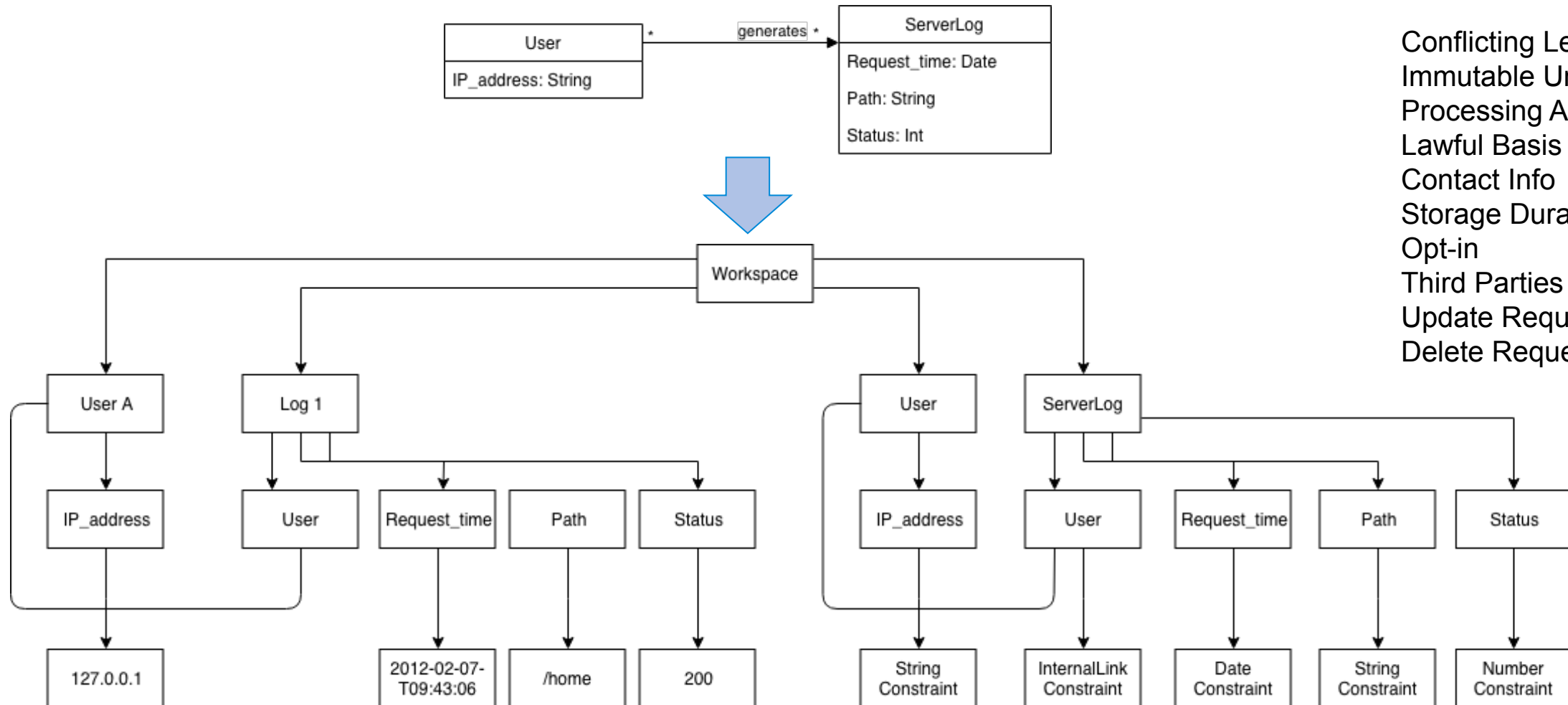


Use Cases

Example 3 Legitimate Interest – IP logging to detect Denial-of-Service attacks

Requirements for GDPR compliance

Conflicting Legislation
Immutable Until
Processing Activity
Lawful Basis
Contact Info
Storage Duration
Opt-in
Third Parties
Update Request
Delete Request



1. Motivation

- GDPR
- Requirements for an Information System
- Hybrid Wikis

2. Research Approach

3. Use Cases

4. Current Progress

5. Timeline

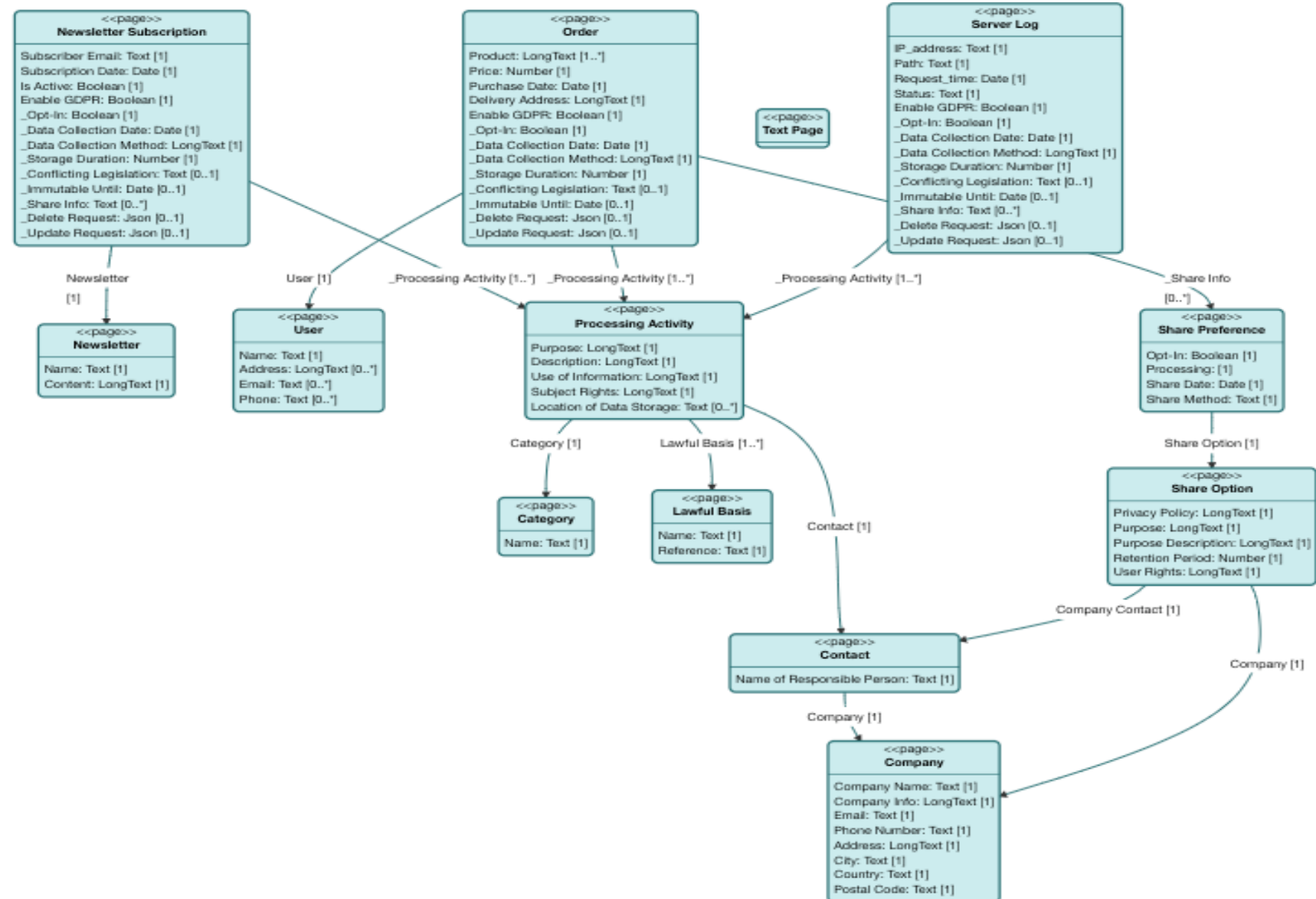
Current Progress

EntityTypes, Entities,
TypeConstraints are created
on SocioCortex Server
based on the use cases

Model requirements for
GDPR compliance are
identified from the use
cases and created proper
attributes, entities and entity
types

Data models are improved
iteratively and incrementally

UML view of GDPR workspace on SocioCortex Server



1. Motivation

- GDPR
- Requirements for an Information System
- Hybrid Wikis

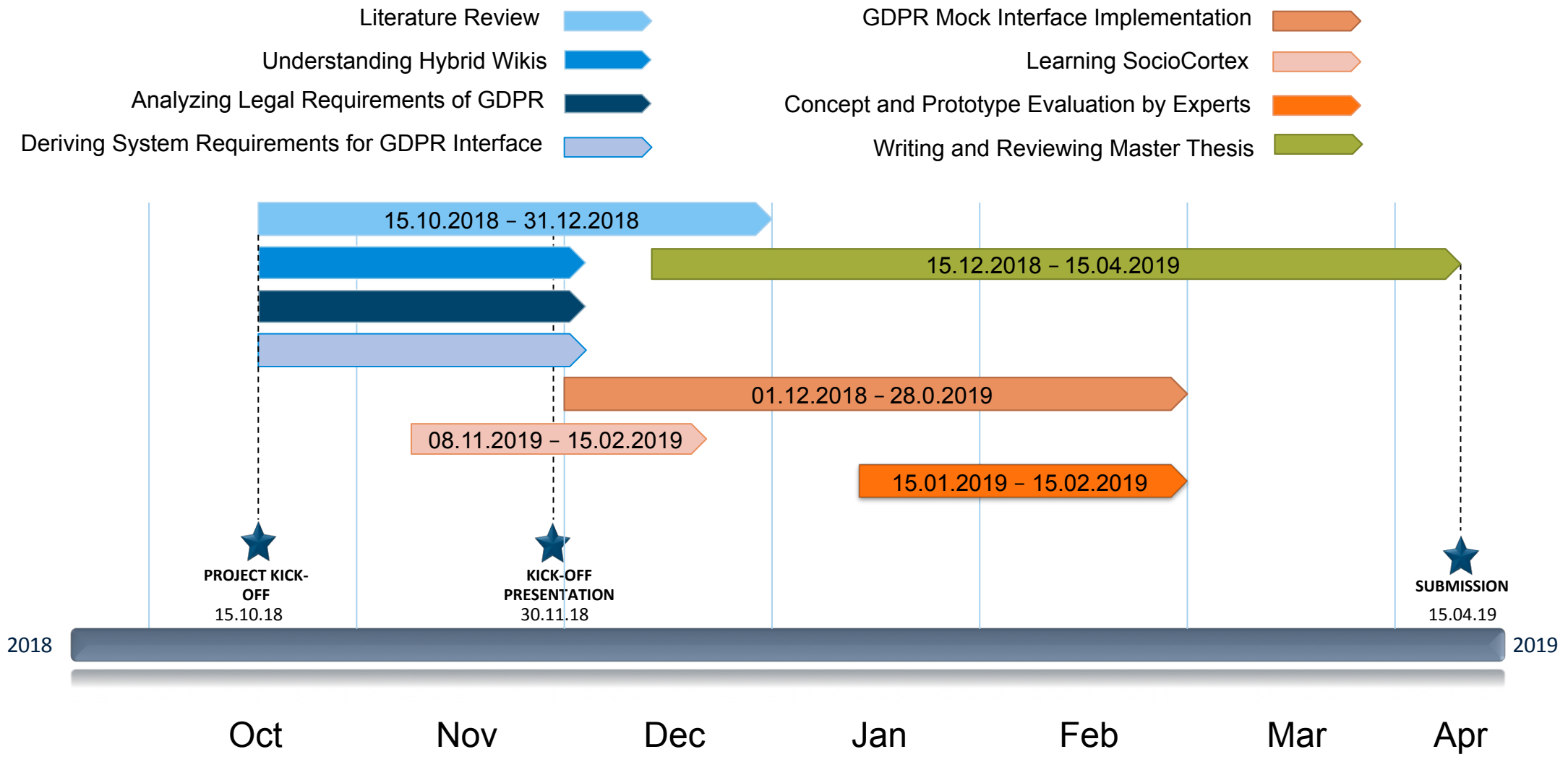
2. Research Approach

3. Use Cases

4. Current Progress

5. Timeline

Timeline





Ahmet Tanakol

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business
Information Systems

Boltzmannstraße 3
85748 Garching bei München

ahmet.tanakol@tum.de
www.matthes.in.tum.de



1. “[EUR_Lex – 32016L0680 – EN – EUR_Lex](#)”. eur-lex.europa.eu. Retrieved 02 November 2018.
2. “[Guide to the General Data Protection Regulation \(GDPR\)](#)”. ico.org.uk. 19 January 2018. Retrieved 02 November 2018.
3. Matthes F.; Neubert C.; Steinhoff A.: Hybrid Wikis: Empowering Users to Collaboratively Structure Information. In: 6th International Conference on Software and Data Technologies (ICSOFT), Seville, 2011
4. Reschenhofer, T.; Bhat, M.; Hernandez-Mendez, A.; Matthes, F.: Lessons Learned in Aligning Data and Model Evolution in Collaborative Information Systems. In: Proceedings of the International Conference on Software Engineering (ICSE), Austin, Texas USA, 2016.