

Master's Thesis: An Information Model as a Basis for Data Gathering to comply with Data Portability according to GDPR Art. 20

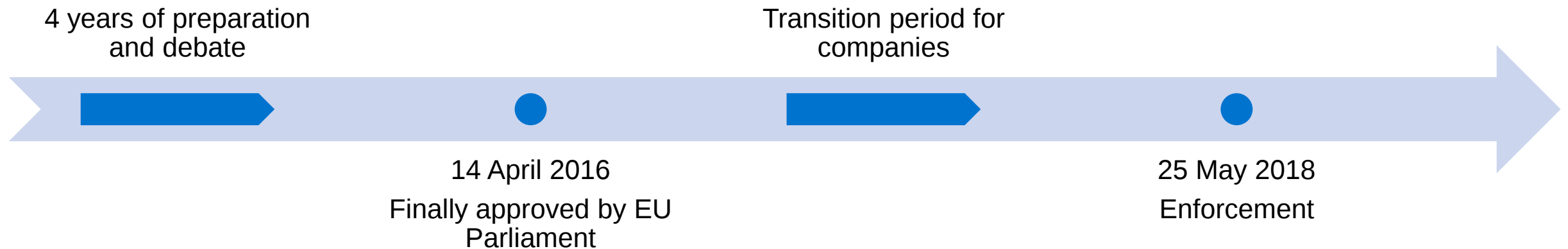
Laura Stojko, 16.11.2018, Final Presentation

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

1. Motivation & Research Outline
2. Requirement Analysis GDPR Art. 20
3. Information Model Development
4. Information Model Evaluation
5. Next Steps

New general data protection regulation (GDPR) [1]

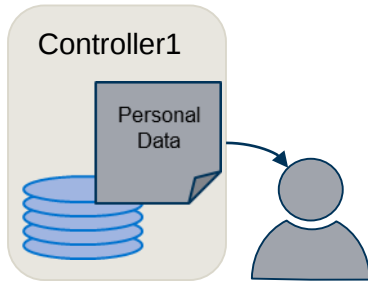
- People have more control over their personal data
- Businesses benefit from a level playing field



Data protection rules for **all companies operating in the EU**

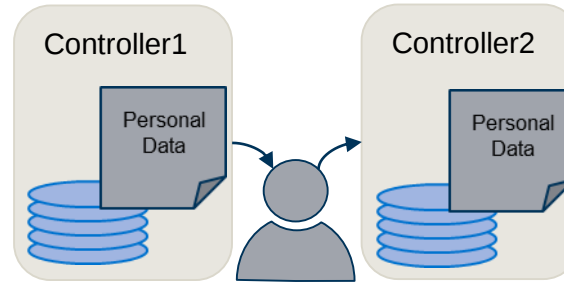
requires

New processes and techniques to meet legal requirements



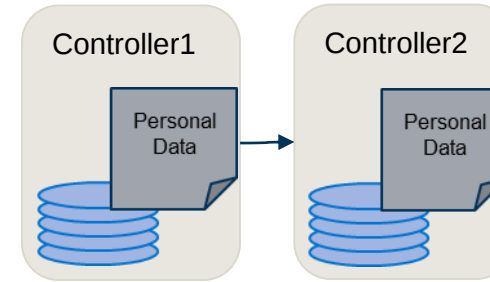
the right to receive

(without hindrance from the data controller) data concerning data subject which he/she has provided (§1);



the right to transmit

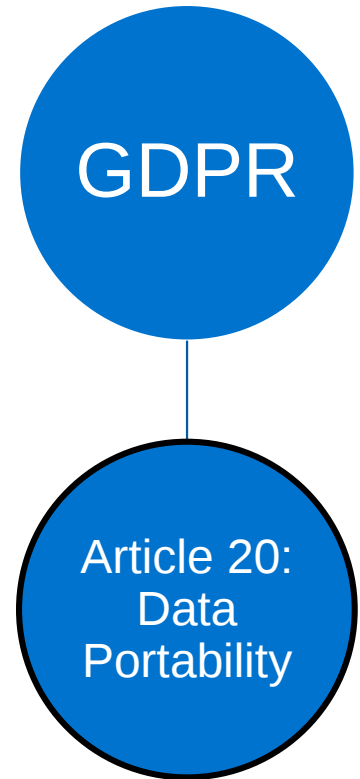
(without hindrance from the data controller) those data to another controller (§1); and



the right to have the personal data transmitted directly

from one controller to another (§2).

[2]

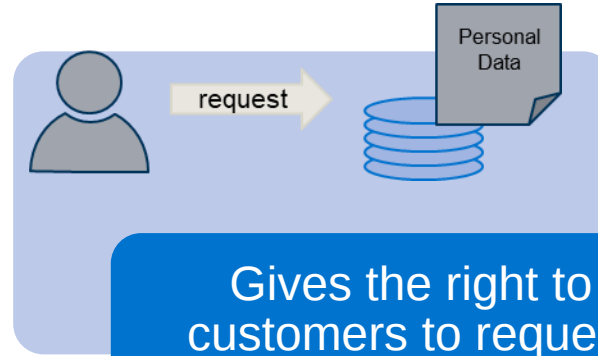


Motivation

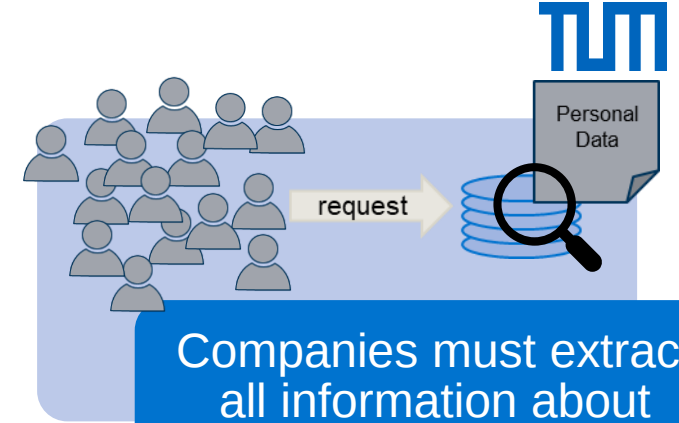
GDPR - Article 20: Data Portability



§ 20 GDPR - Data Portability



Gives the right to customers to request reports about stored personal data, data usage and handling



Companies must extract all information about requester and give additional information about data usage

Research Goal:

Development of an information model that enables a service for data collection to comply with GDPR Art. 20

Research Goal:
Development of an information model that enables a service for data collection to comply with GDPR Art. 20



What are existing approaches of information models?



What are the requirements for fulfilment of GDPR Art. 20?

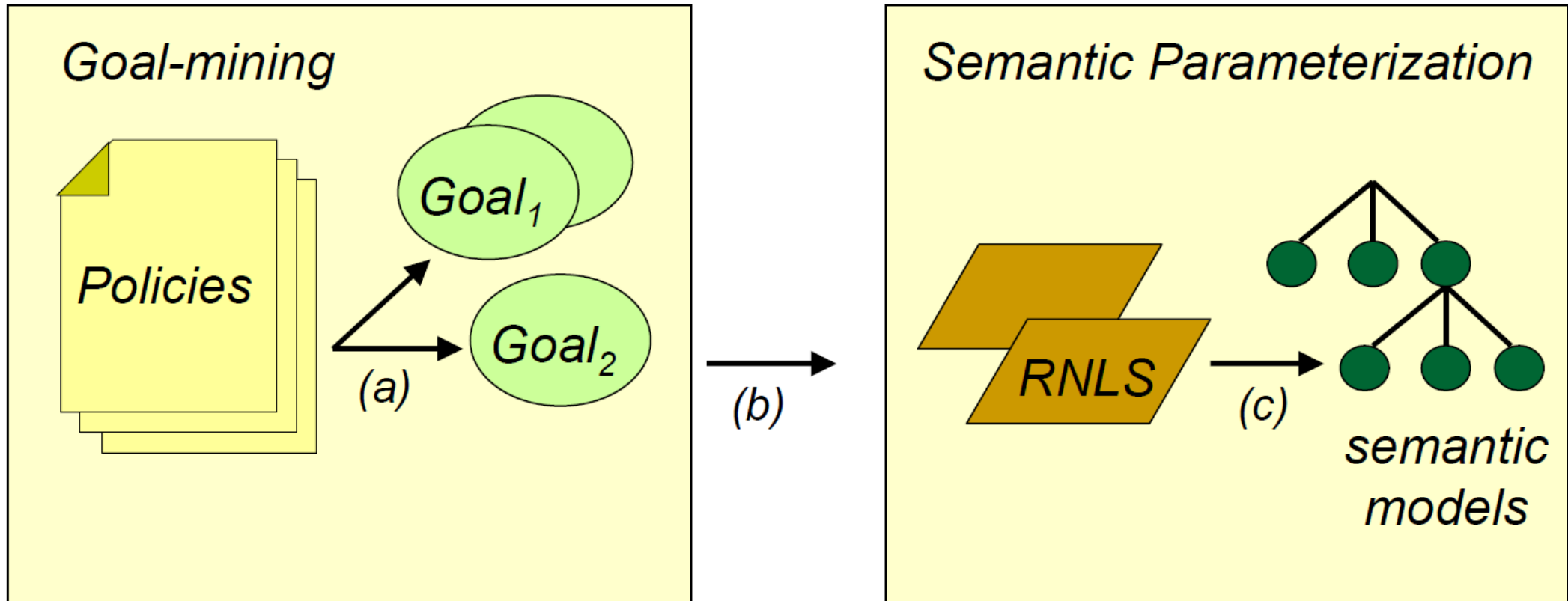


What is a possible information model for business objects covering the requirements of GDPR Art. 20?



How useful and applicable is the developed information model?

1. Motivation & Research Outline
2. Requirement Analysis GDPR Art. 20
3. Information Model Development
4. Information Model Evaluation
5. Next Steps



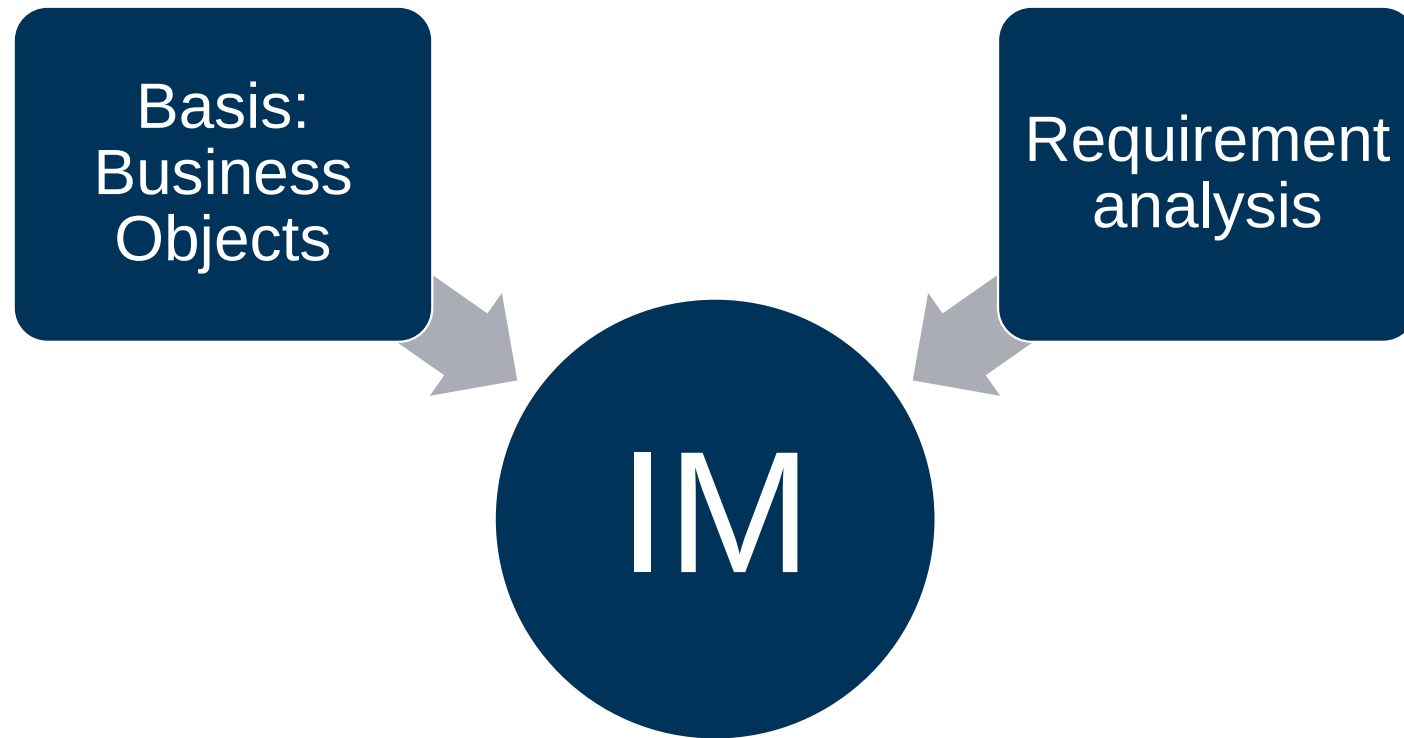
(a) Goals are mined from policies.

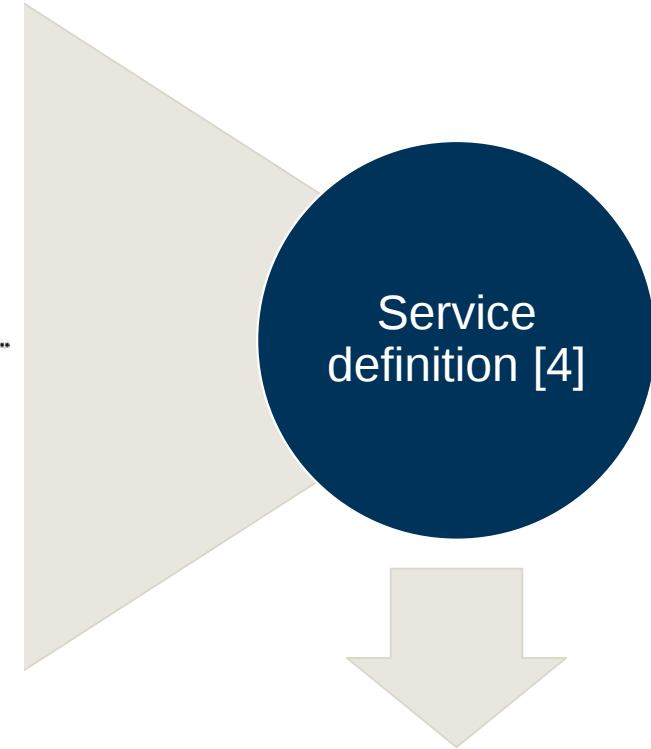
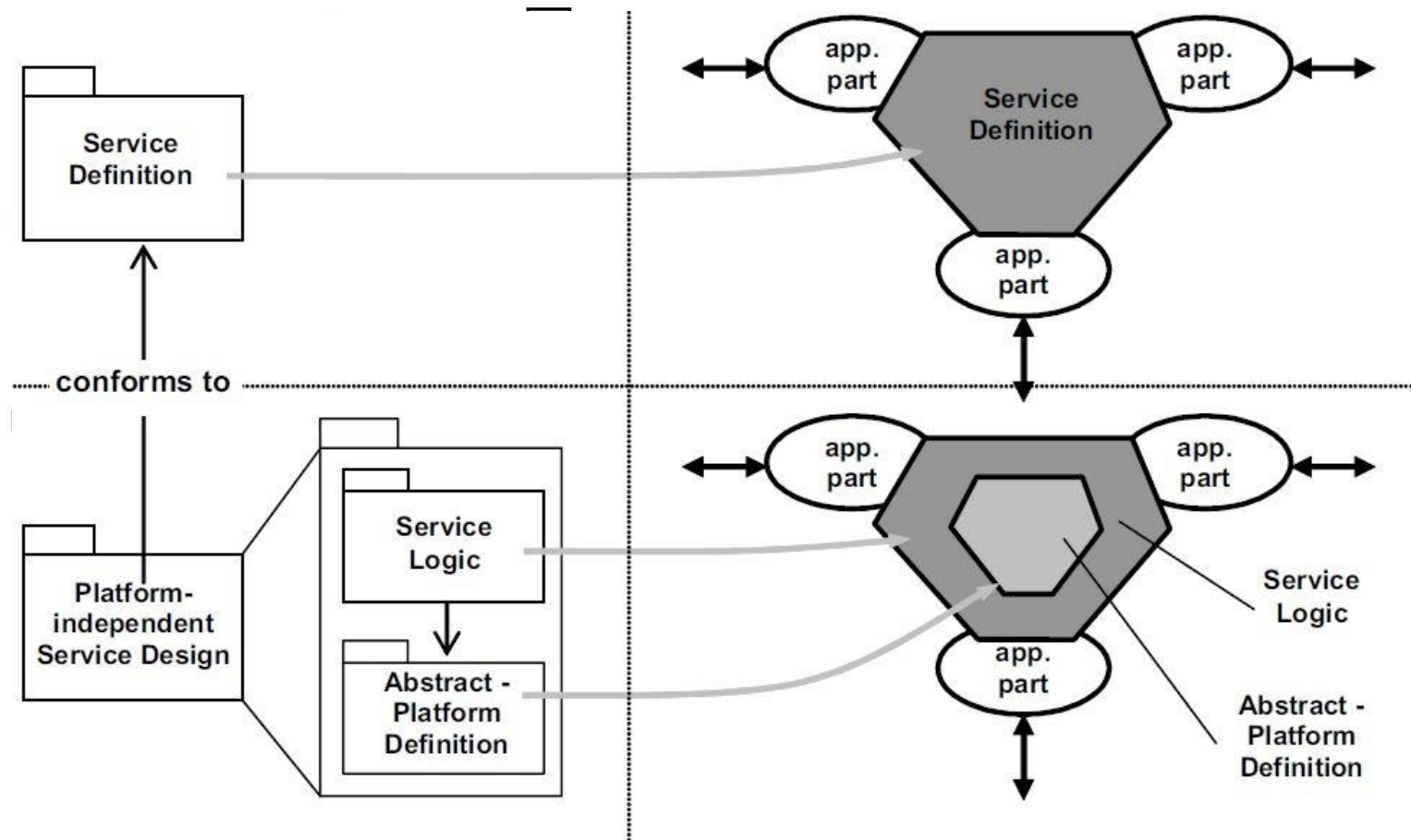
(b) Restate goals as Restricted Natural Language Statements (RNLS).

(c) RNLS are parameterized to build semantic models.

Required information	GDPR source
personal data concerning the data subject	Data Portability (Art. 20)
consent pursuant	Lawfulness of processing (Art. 6 (1 a, b))
explicit consent pursuant	Processing of special categories of personal data (Art. 9 (2 a))
specific categories of personal data	Processing of special categories of personal data (Art. 9 (2 a))
contract pursuant	Data Portability (Art. 20)
erasure date	Right to Erasure (Art. 17)
public interest	Right to Erasure (Art. 17)

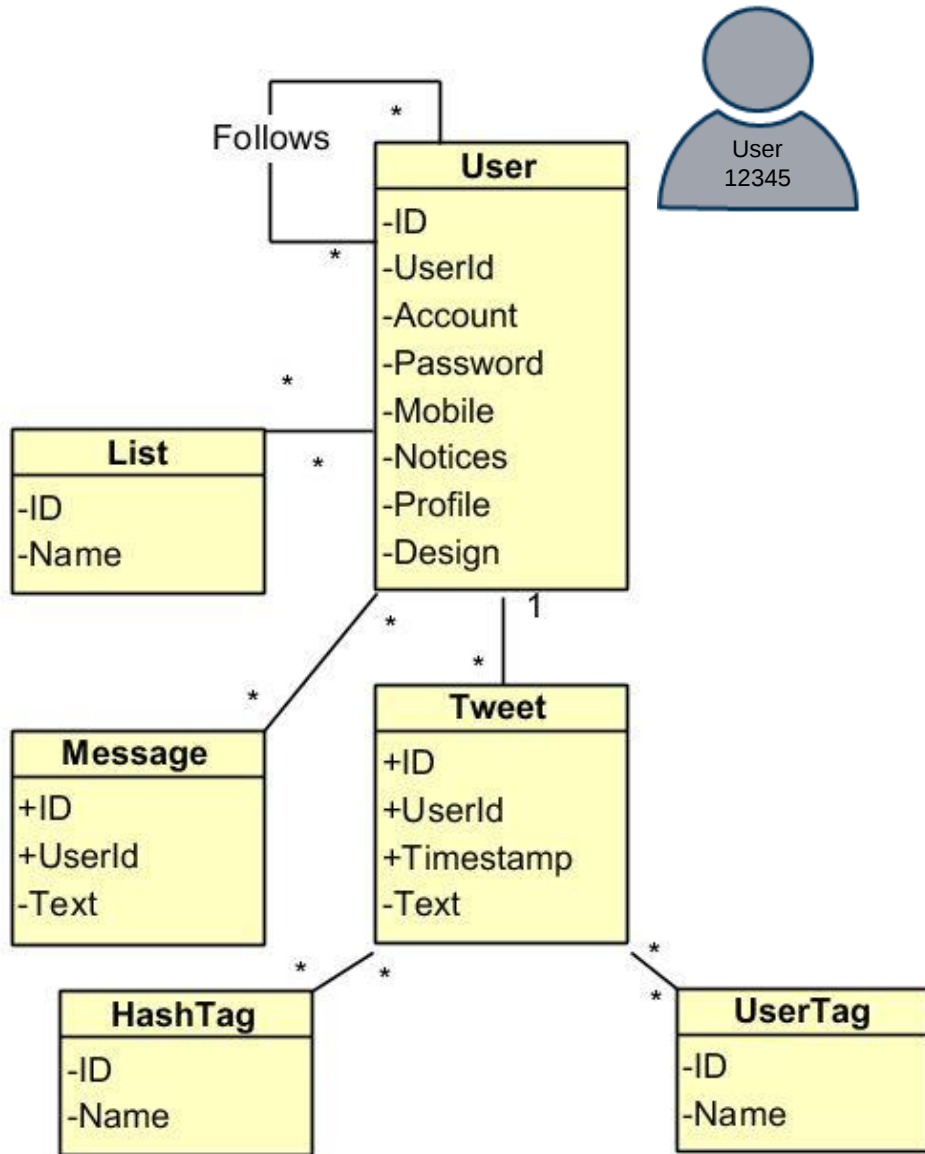
1. Motivation & Research Outline
2. Requirement Analysis GDPR Art. 20
3. Information Model Development
4. Information Model Evaluation
5. Next Steps



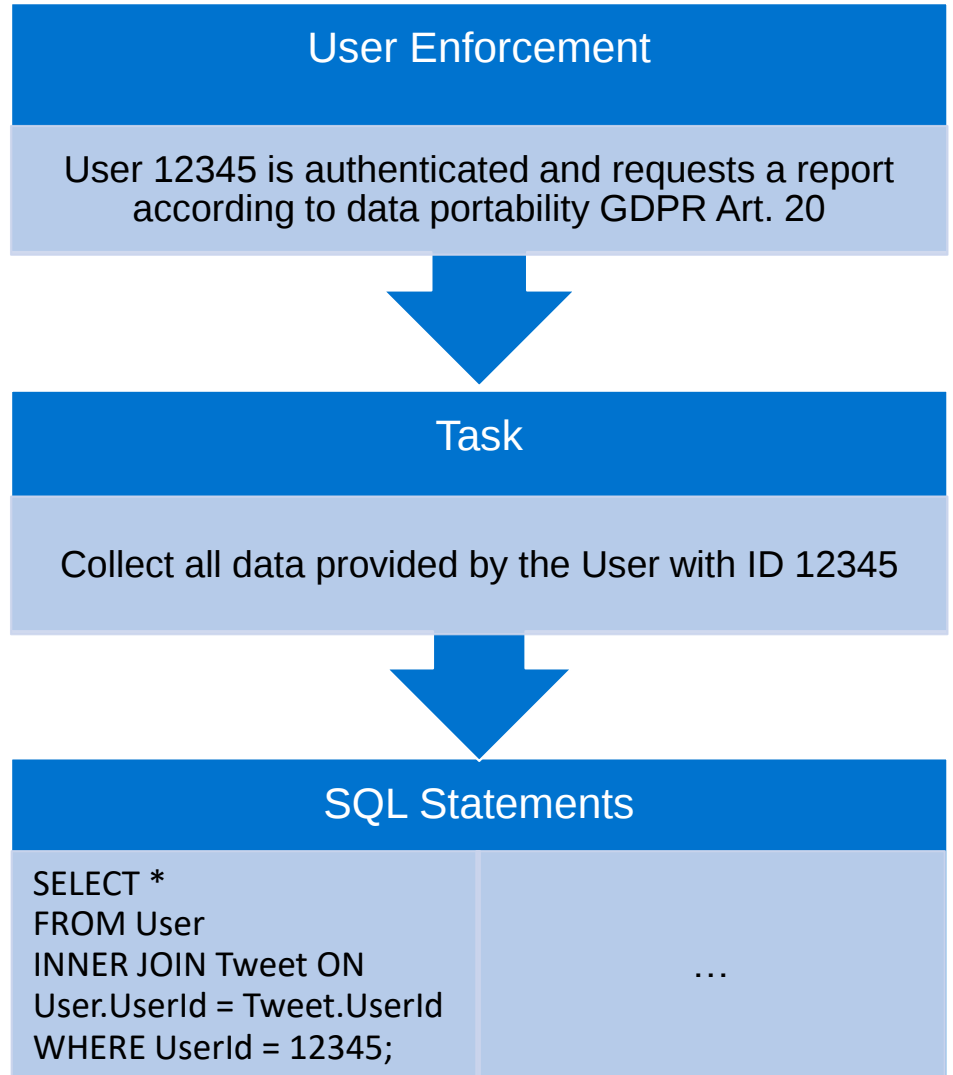


An IM independent of company, industry or platform

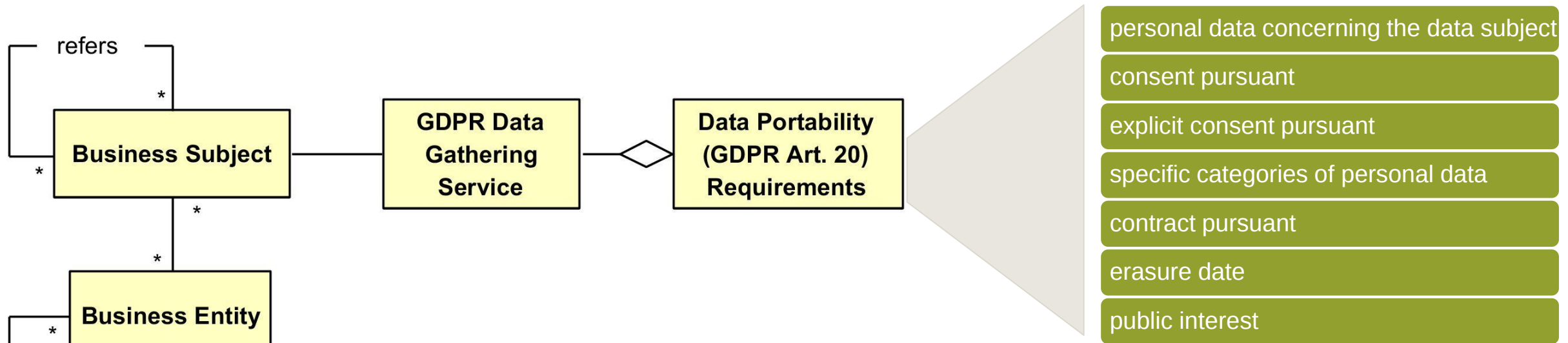
Final Information Model – Twitter Example



[8]



Final Information Model



Business Subject:

- A Business Subject is a type of business object which is stored as master data. Examples for a Business Subject are product records or customer records. For this thesis, Business Subjects which are directly related to a person, like a customers record, are in focus.

Business Entity:

- A Business Entity is a type of business object which is created by and directly connected to a Business Subject, in other words transaction data (e.g. invoices, orders).

GDPR Data Gathering Service:

- This service is an integration layer which requests data sources for the required information for the data transfer and consolidates the results.

Data Portability (GDPR Art. 20) Requirements

- This class provides a list of information which are necessary to fulfill data portability. It is the basis for the GDPR Data Gathering Service, as it provides the properties the service queries.

1. Motivation & Research Outline
2. Requirement Analysis GDPR Art. 20
3. Information Model Development
4. Information Model Evaluation
5. Next Steps

#	Current profession	Company size	Industry
1	Cyber Security Portfolio Manager	large enterprise	Industrial manufacturing
2	Head of IT Strategy	large enterprise	Industrial manufacturing
3	Co-Founder Compliance tool	Start-Up	IT service and consulting
4	Corporate Data Privacy Officer	large enterprise	Industrial manufacturing
5	Cyber Security Architect	large enterprise	Industrial manufacturing
6	Head of Sales for privacy management tool	SME	IT service and consulting
7	Business Intelligence (2)	large enterprise	Finance

Expert Interviews – Evaluation of the Information Model according to Lindland et al. criteria:

based on the sign theory and is developed for conceptual models like data models, process models, interaction models etc.

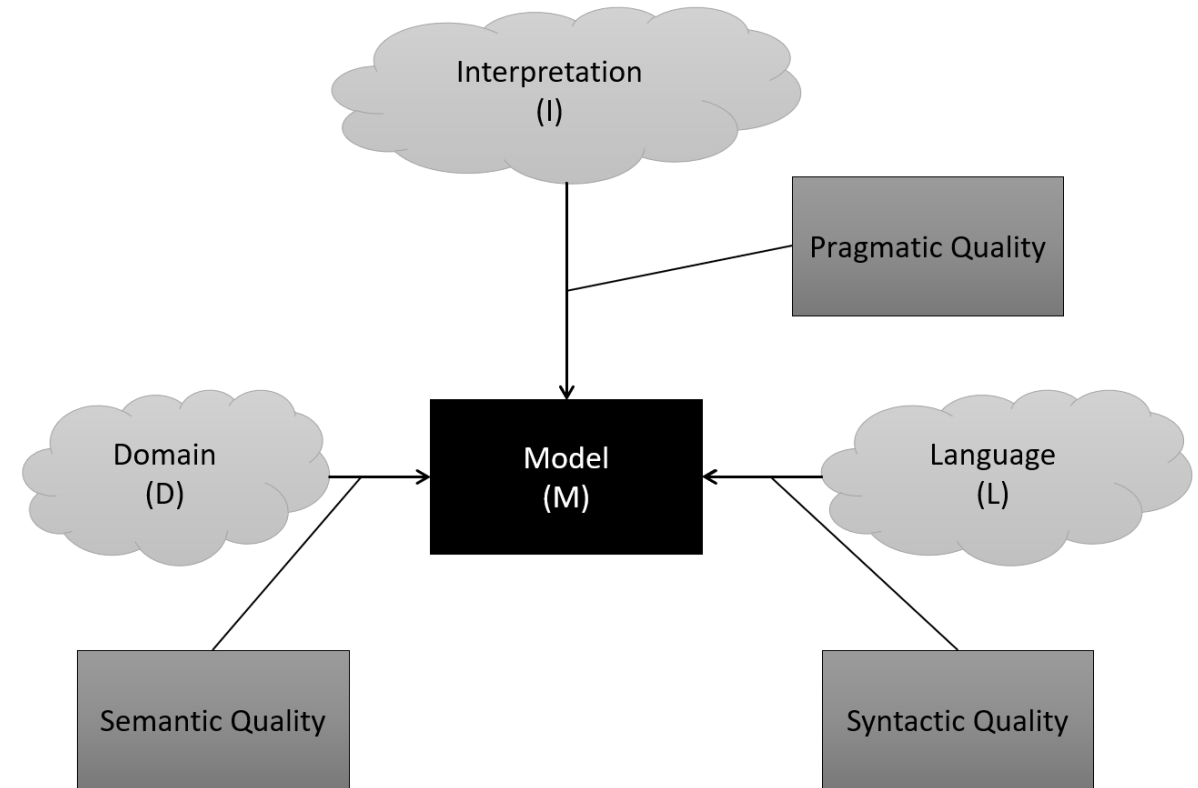
Syntactic quality: realization of the modelling language used within the model. (only use statements which are syntactic correct)

Semantic quality: validity and completeness of the model with respect to the problem domain.

Pragmatic quality: the interpretation of the model by the stakeholders and the objective of comprehensibility.

The evaluation of Lindland et al. [6] proposed quality framework by Moody et al. [7] determines the framework as

'valid, with the quality categories found to be necessary, sufficient and independent.'



Expert's opinion regarding **information model**:



Advantages

- Syntactic and semantic quality improved iteratively with the interviews (complete, valid information model)
- Distinction master data and transaction data
- Usefulness: greenfield approach / guidance for companies with complex structures
- Implementation ideas (DWH, EDI)
- Abstraction level is right as querying databases is platform specific

Disadvantages

- Pragmatic quality: Interpretation of the model is difficult as no implementation details are provided
- Companies need to identify where their data is stored and how to access it (e.g. CMD)

Expert's opinion regarding **data portability**:



Advantages

- Data portability is seen as highly relevant for customers
- Market entry opportunity for small companies – level playing field
- New possibilities for data trading

Disadvantages

- Standard for data portability is required
- Non-existing information about how to handle back-ups and references of personal data
- Data stored about a person more interesting than portability
- Cost-relation analysis will often show that implementation is not suitable
- Companies only invest minimal effort for compliance

Expert's opinion regarding **GDPR**:



Advantages

- Homogeneous data privacy law in Europe
- Higher awareness of data privacy

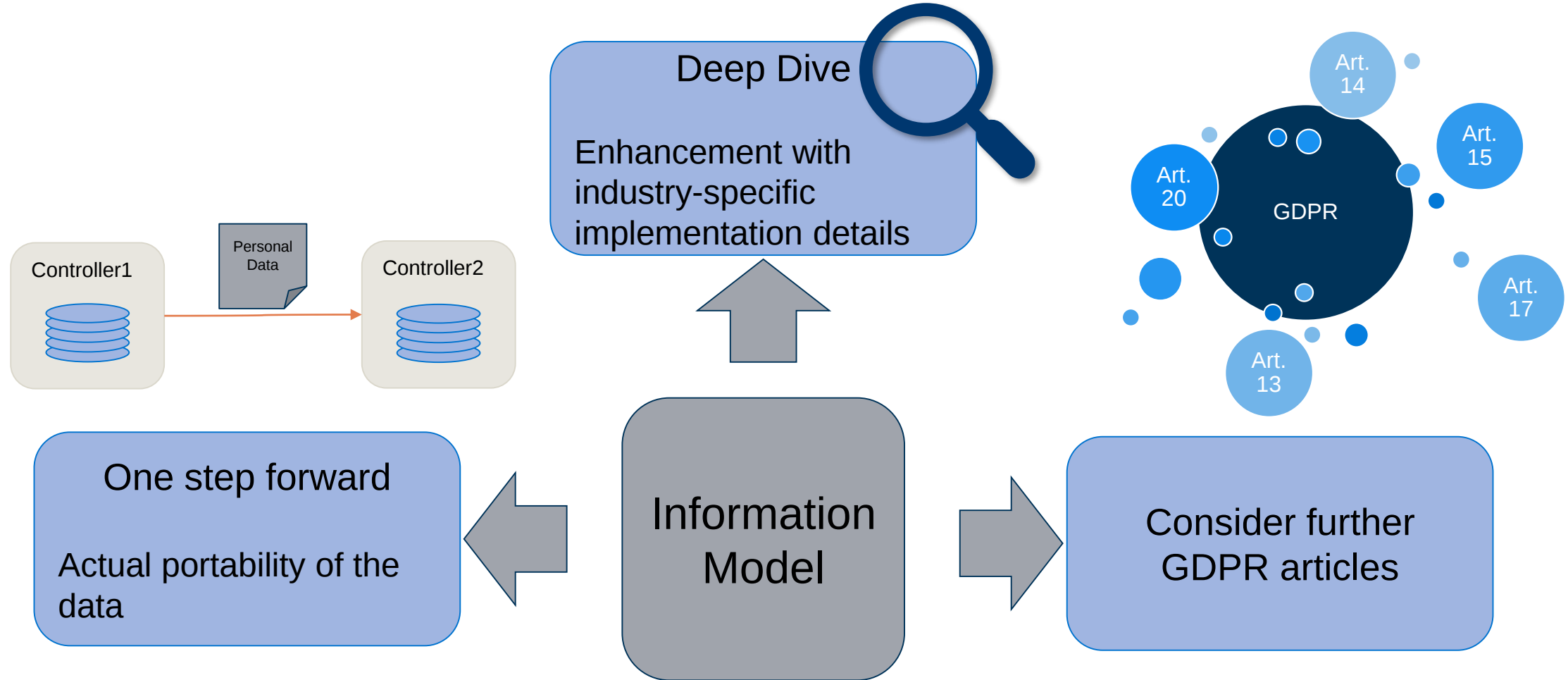


Disadvantages

- Companies try to profit from GDPR (consent to more processing activities)
- People do not know how to enforce their right correctly
- GDPR scope is too broad – not limited to services for information society
- People do not know their correct legal basis

1. Motivation & Research Outline
2. Requirement Analysis GDPR Art. 20
3. Information Model Development
4. Information Model Evaluation
5. Next Steps

Next Steps – Information Model Enhancements





B.Sc.

Laura Stojko

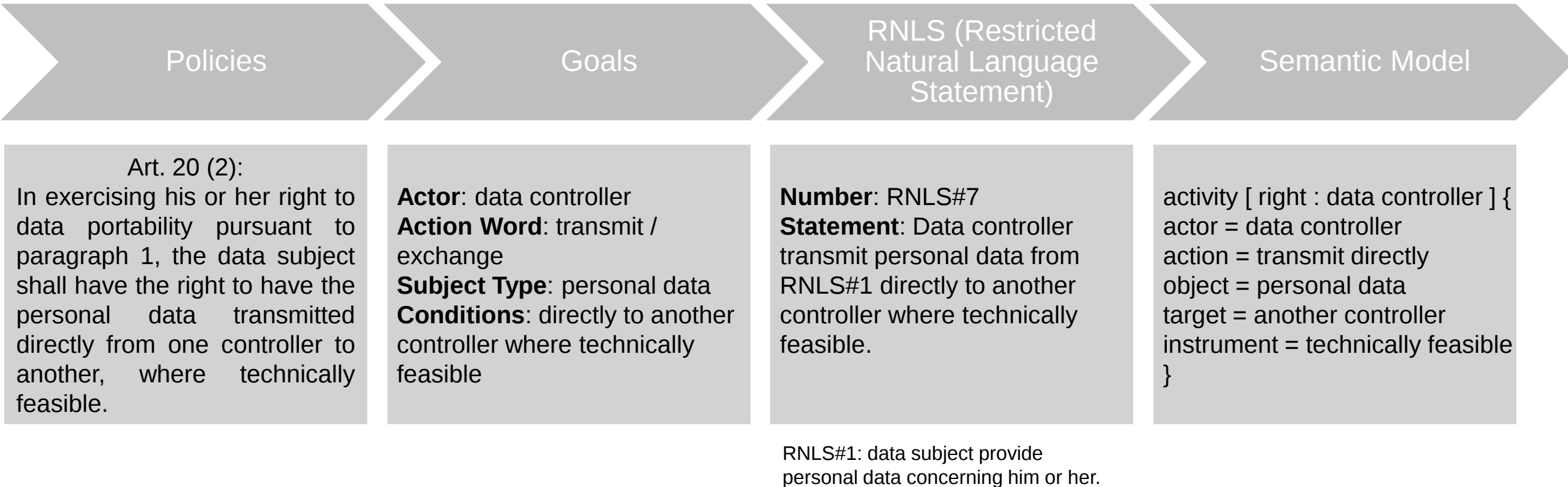
Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business
Information Systems

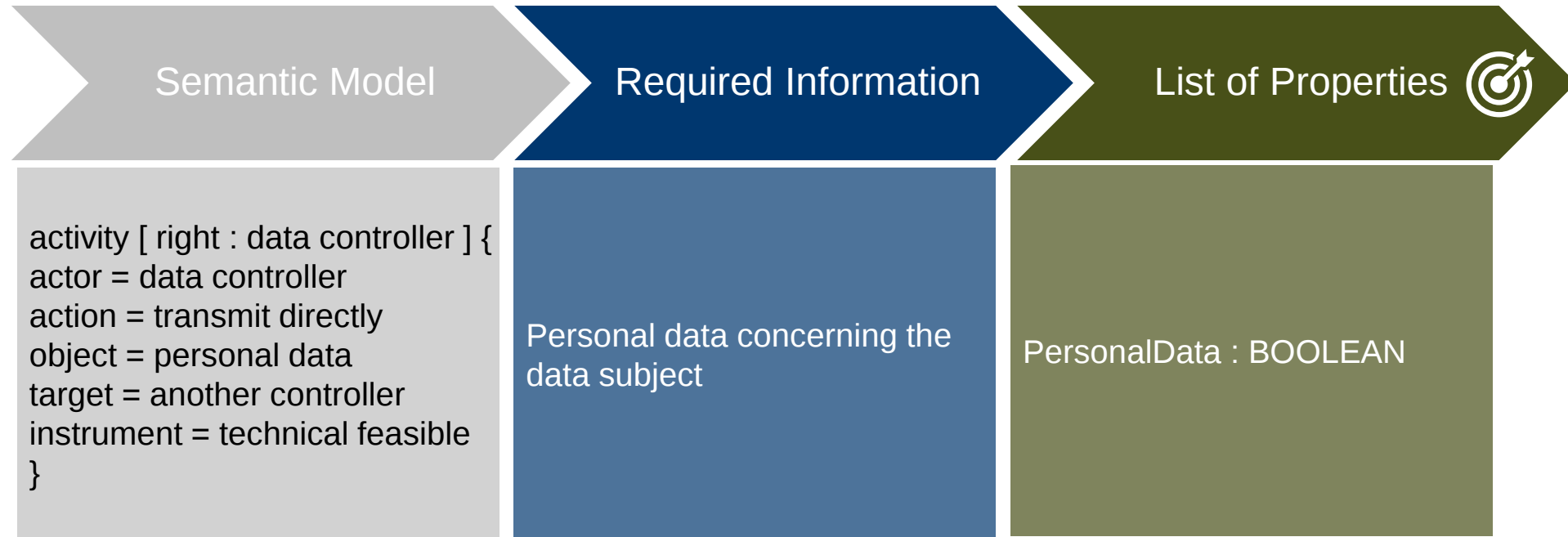
Boltzmannstraße 3
85748 Garching bei München

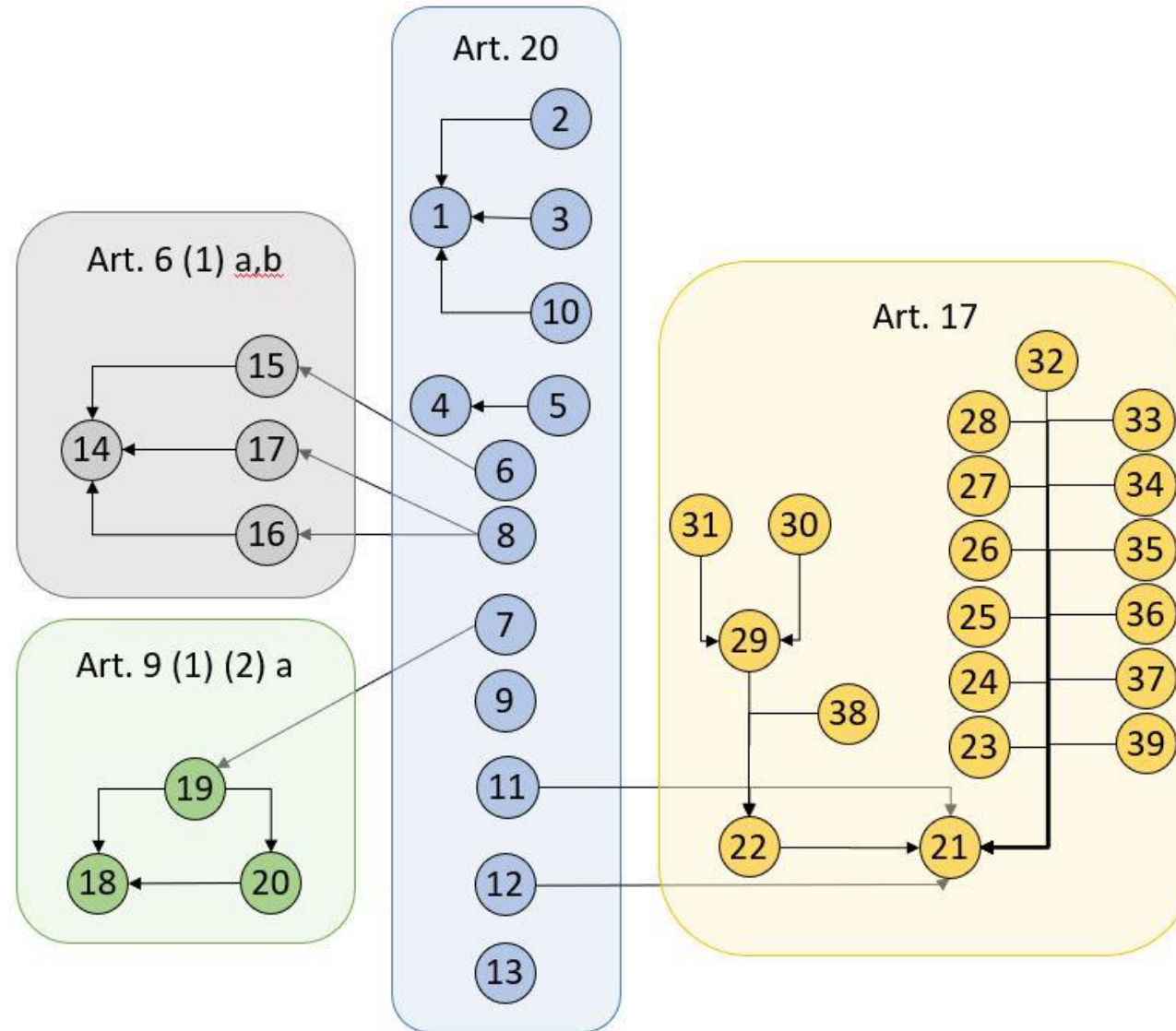
laura.stojko@tum.de
www.matthes.in.tum.de



- [1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119 (4 May 2016), pp. 1-88, 2016.
- [2] De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, 34(2), 193–203. <https://doi.org/10.1016/J.CLSR.2017.10.003>
- [3] Breaux, T. D., & Antón, A. I. (2005). Analyzing Goal Semantics for Rights, Permissions and Obligations Presentation Outline Towards Machine-enforceable Policies Motivations. Retrieved from <https://www.cs.cmu.edu/~breaux/presentations/tdbreaux-re05.pdf>
- [4] João Paulo Almeida, Marten Van Sinderen, Luís Ferreira Pires, and Dick Quartel. A systematic approach to platform-independent design based on the service concept. *Proceedings - 7th IEEE International Enterprise Distributed Object Computing Conference*, 2003-Janua(January):112–123, 2003. doi:10.1109/EDOC.2003.1233842.
- [5] Reinhard Schütte. Die neuen Grundsätze ordnungsmäßiger Modellierung. In *Grundsätze ordnungsmäßiger Referenzmodellierung*. Gabler Verlag, Wiesbaden, 1998. URL: http://link.springer.com/10.1007/978-3-663-10233-5_3, doi:10.1007/978-3-663-10233-5_3.
- [6] O.I. Lindland, G. Sindre, and A. Solvberg. Understanding quality in conceptual modeling. *IEEE Software*, 11(2):42–49, mar 1994.
- [7] D.L. Moody, G. Sindre, T. Brasethvik, and A. Solvberg. Evaluating the quality of information models: empirical testing of a conceptual model quality framework. In *25th International Conference on Software Engineering*, 2003. *Proceedings.*, pages 295–305. IEEE, 2003
- [8] Matthijs Neppelenbroek, Matthias Lossek, and Rik Janssen. Twitter: An architectural review. *Scholars paper on Software Architecture at Utrecht University*, 2011. URL: http://www.timdeboer.eu/paper_publishing/Twitter_An_Architectural_Review.pdf.









‘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;

Article 4:
Definitions
– Personal
Data

GDPR

Article 20:
Data
Portability

