Bachelor Thesis Kick Off | State of the Art in linking privacy requirements to technical solutions

Nora Miftah El Kheir, 16.11.18, Garching

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

Outline

Motivation

On the 25.05.18 the General Data Protection Regulation (GDPR) came into effect

It regulates the data protection and privacy for all companies operating in the European Union

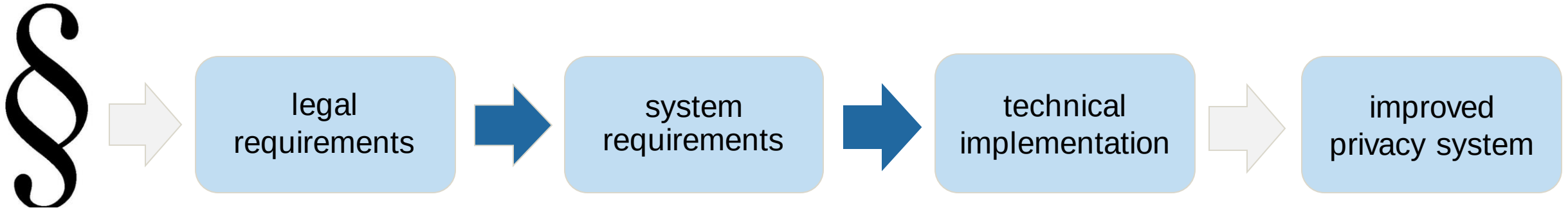
Non-compliance could result in high fines

Challenges: the regulation is formulated as an open norm and doesn`t consist of concrete suggestions how to implement the legal requirements

Motivation
Example: Art. 5 GDPR 1a

"Personal data shall be processed in a manner that ensures **appropriate** security of the **personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using **appropriate** technical or organisational measures "

Generalized Process



Outline

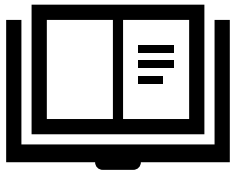
1. Motivation

2. Research Questions and Approach

3. First Results

4. Timeline

Research Questions



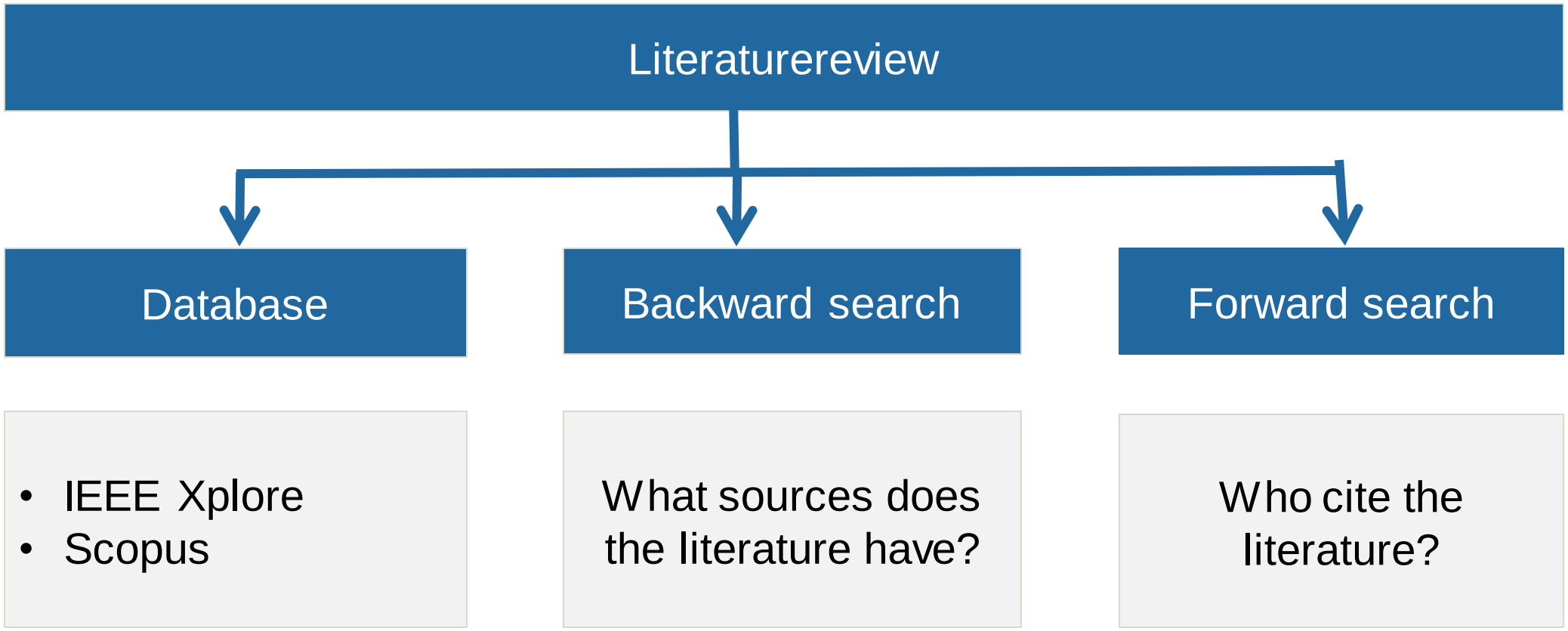
RQ1: What is the state of the Art in linking privacy requirements to technical solutions and which categories make it possible to classify the frameworks?

RQ2: Which research methods were used and how were they applied?

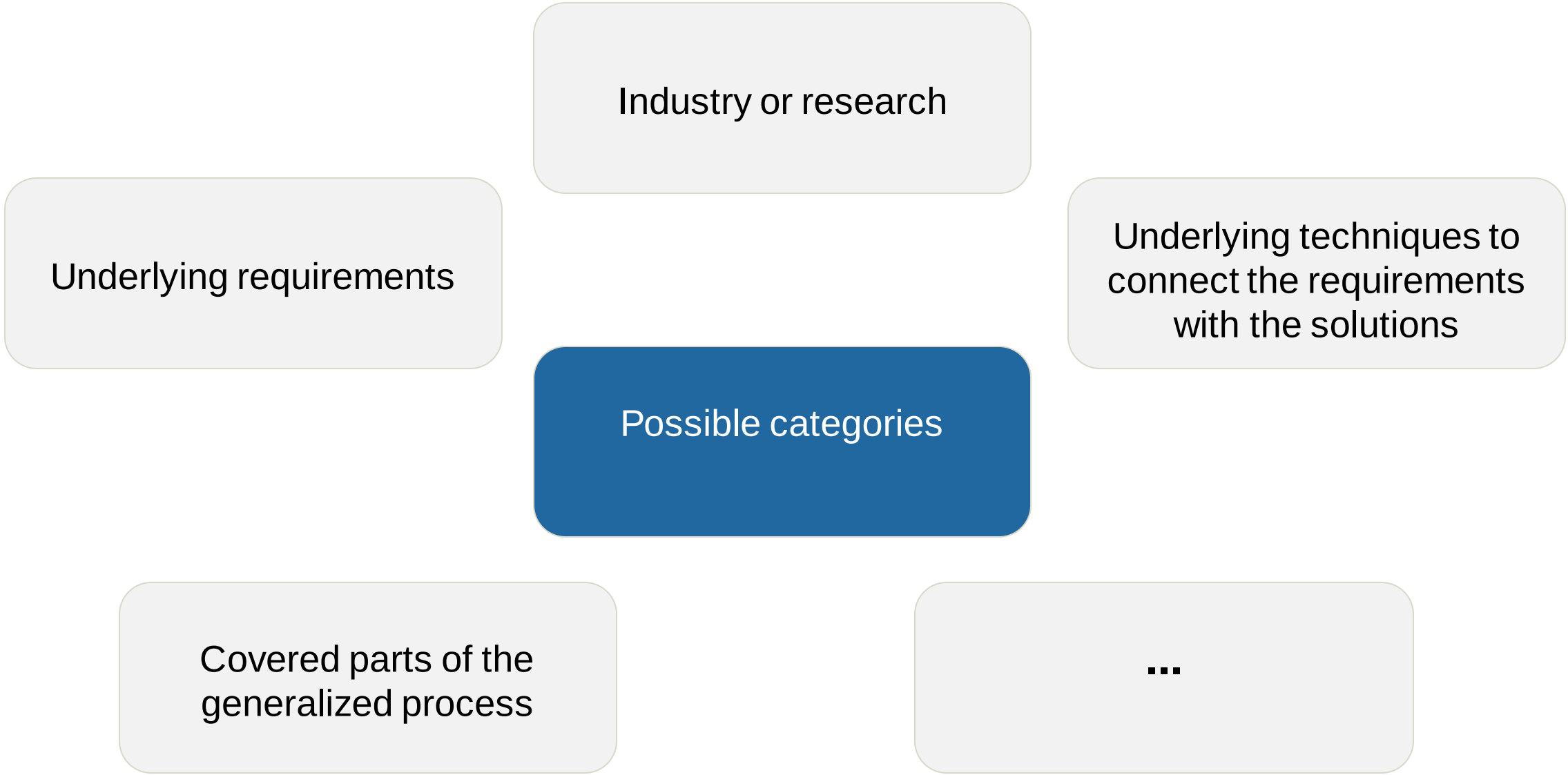
RQ3: How far are these methods applied in practice?

RQ1: Literaturereview

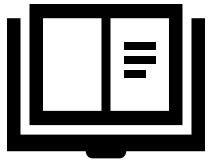
- Based on Kitchenham [1]



RQ1: Categorization of the frameworks



Research Questions



RQ1: What is the state of the Art in linking privacy requirements to technical solutions and which categories make it possible to classify the frameworks?

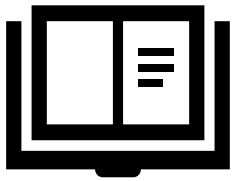
RQ2: Which research methods were used and how were they applied?

RQ3: How far are these methods applied in practice?

RQ2: Design Science Process

[2]

Research Questions



RQ1: What is the state of the Art in linking privacy requirements to technical solutions and which categories make it possible to classify the frameworks?

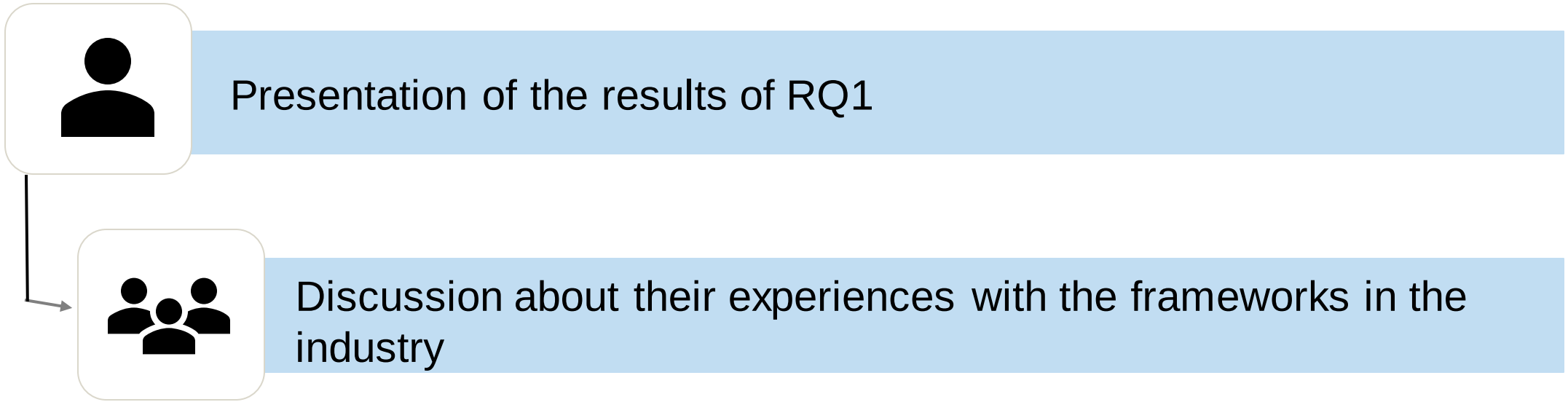
RQ2: Which research methods were used and how were they applied?

RQ3: How far are these methods applied in practice?

RQ3: Workshop

- Conduction of a workshop with industrial partners
- Expected date: end of January

Workshop process:



Outline

1. Motivation

2. Research Questions and Approach

3. First Results

4. Timeline

Data Collection

Used databases: Scopus, IEEE Xplore

Step	Search with search term	Filter	Delete duplicate articels	Relevant titles	Relevant abstracts	Forward & Backward search
Amount of papers	313	220	215	35	11	8

19 relevant paper

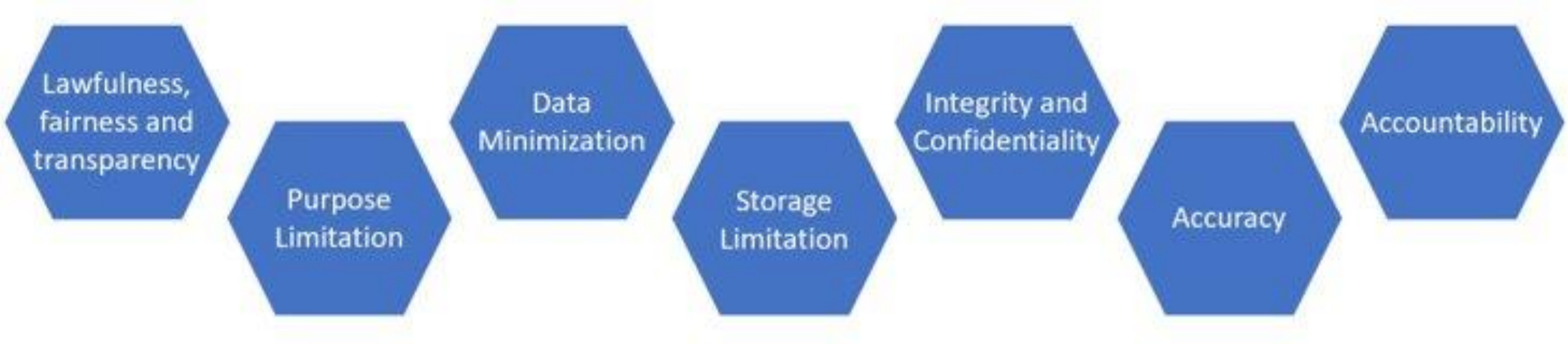
Relevant Paper

Data protection by design in systems development: From legal requirements to technical solutions
Legal Requirements, Compliance and Practice: An Industry Case Study in Accessibility
PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology
Experiences in the Development and Usage of a Privacy Requirements Framework
A Critical Analysis of Privacy Design Strategies
Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering
Impact of Legal Interpretation in Business Process Compliance
A process for data protection impact assessment under the European GDPR
Privacy by design: From research and policy to practice – the challenge of multi-disciplinarity
Supporting privacy by design using privacy process patterns
Addressing privacy requirements in system design: The PriS method
Checking existing requirements for compliance with law using a production rule model
Privacy and Data Protection by Design-from policy to engineering
Comparing Privacy Requirements Engineering Approaches
Towards a principled approach for engineering privacy by design
A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy req.
Pris methodology: incorporating privacy requirements into the system design process
How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns
Engineering Privacy

Paper 1: Data Protection by Design in Systems Development: From legal requirements to technical solutions

by F. Blix; S. A. Elshekeil; S. Laoyookhong

Requirements for the framework:



DPP1: Lawfulness, Fairness and transparency

GDPR Provision

"processed lawfully, fairly and in a transparent manner in relation to the data subject"
GDPR Art.5.1(a)

Objective

Processing of personal data no matter how minor the processing is has to stand on a firm legal basis. The data controllers have to provide clear views on how the processing works and the consequences on the data subject before collecting and processing the data.

Organizational Measures

Strategy: embed privacy into the organization strategy to demonstrate strong commitment to privacy

Policies, processes, and procedures: to assess, manage the lawfulness and the adherence to the legal requirements at all stages of the data processing. This includes the roles and responsibilities of different individuals involved in the data processing

Legal Measures: clear guidelines and measure of selecting, enforcing and documenting the right legal bases of the processing

Technical Measures

Embedded Transparency Measures: embedding necessary forms, dialogues, notifications into information systems. Such as asking for consent before collecting location data of a mobile app user

Embedded Legal Measures: For example, an embedded database that capture consents from users of the information system, and map it to the user data. This can help the users to exercise their rights and the organization to manage their obligations

Non-Repudiation Services: Implementing the non-repudiation service from the data subject. For example, the digital signatures shall be implemented when the collected data is sensitive.

[3]

Outline

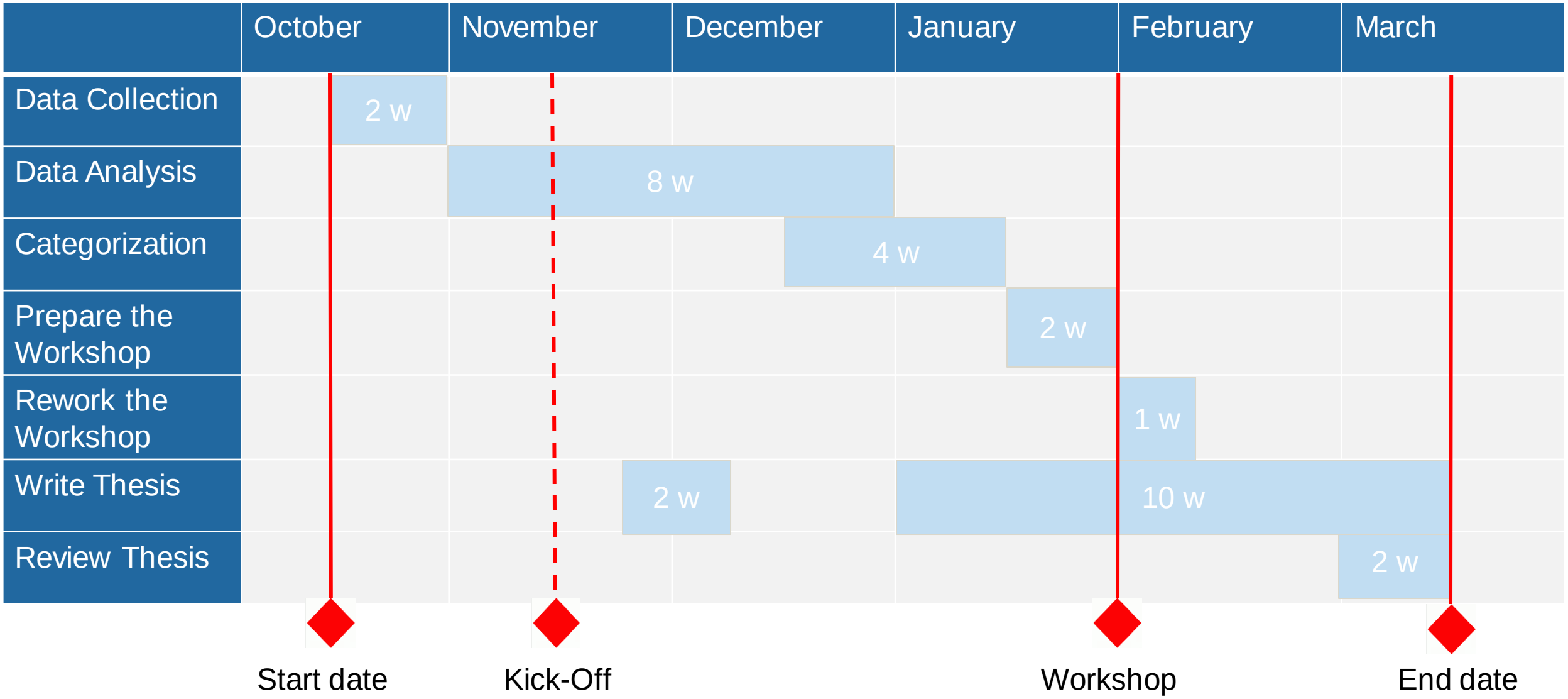
1. Motivation

2. Research Questions and Approach

3. First Results

4. Timeline

Timeline



References

[1]Barbara Kitchenham. 2004. Procedures for Performing Systematic Reviews

[2] Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007.
A Design Science Research Methodology for Information Systems Research,

[3] Fredrik Blix, Salah Addin Elshekeil, Saran Laoyookhong. 2017. Data Protection by Design in Systems Development – From legal requirements to technical solutions

[4] Salah Addin Elshekeil, Saran Laoyookhong. 2017. Data Protection by Design in Systems Development – From legal requirements to technical solutions

Nora Miftah El Kheir

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

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.
Fax +49.89.289.17136

nora.miftah@web.de
wwwmatthes.in.tum.de