# Bachelor’s Thesis Kick-Off: Empirical Task Analysis of Data Protection Management

Michael Vilser 5.06.2019

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

# Key Facts

**Title:** Empirical Task Analysis of Data Protection Management

**Author:** Michael Vilser

**Advisor:** Dipl. Math.oec. Dominik Huth

**Supervisor:** Prof. Dr. Florian Matthes

**Start:** June 15th, 2019

**End:** November 15th , 2019

# Outline

- Motivation
- Problem Statement
- Research Questions
- Approach
- Next Steps


© sebis

# Motivation

**General Data [1] Protection Regulation**

1. Transparent Processing
2. Limitation of purpose
3. Data subject rights
4. …

**On violation:**
Fine up to €20M or 4% of the worldwide annual revenue

**Appointment of a Data Protection Officer**

**Constant evaluation of GDPR compliance**

**Maintaining a record of processing activities**



© sebis

# Motivation

**Enterprise Architecture Management**

*Enterprise Architect*

**Shared Requirements [2]:**

- Overview of the organization
- Understanding of processes, applications and dataflows
- A vocabulary and model for abstraction
- Method to obtain consistent and reproducible results

**Data Protection Management**

*Data Protection Officer*


© sebis

# Problem Statement

## Previous Research

Deductive approach based on [2][3]

- Design Science Research
- Content analysis of the GDPR
- EAM literature and models

Enterprise Architecture Models/Extensions
for GDPR compliance

**BUT**
Rather EAM centric
Generalizability?
Actual Use?


© sebis

# Research Questions

RQ1) What activities in Data Protection Management are necessary to achieve GDPR compliance?

RQ2) Which problems occur while performing these activities?

RQ3) How are DPOs collaborating with EAM at the moment and how helpful is it?


© sebis

# Approach – Desired outcome

| **Activities**<br>**(also rated in terms of complexity and time consumption)** | **Problems** | **Already supported by EAM? How helpful is it?** | **Should Data Protection Management get supported by EAM in the future?** |
|---|---|---|---|
| Activity A<br>• Time consumption<br>• Complexity | Problem 1<br>Problem 3 | No<br>-> Reasons? | Yes/No |
| Activity B<br>• Time consumption<br>• Complexity | Problem 2<br>Problem 4<br>Problem 5 | Yes – very helpful | Yes |
| Activity C<br>• Time consumption<br>• Complexity | Problem 2 | Yes – not very helpful | No |
| … | … | … | … |


© sebis

# Approach

## Literature Research

- GDPR compliance using EAM [2][3]
- Tasks & Responsibilities of DPOs [4]
- Monetary value

## Interviews with DPOs

- Enhance domain knowledge
- Verify survey

## Survey preparation

- Question design
- Participant acquisition via Xing, LinkedIn, bvdnet.de, personal Contacts

## Survey execution

- Planned duration: 15.August to 30.September

## Evaluation

- Statistics
- Recommendations

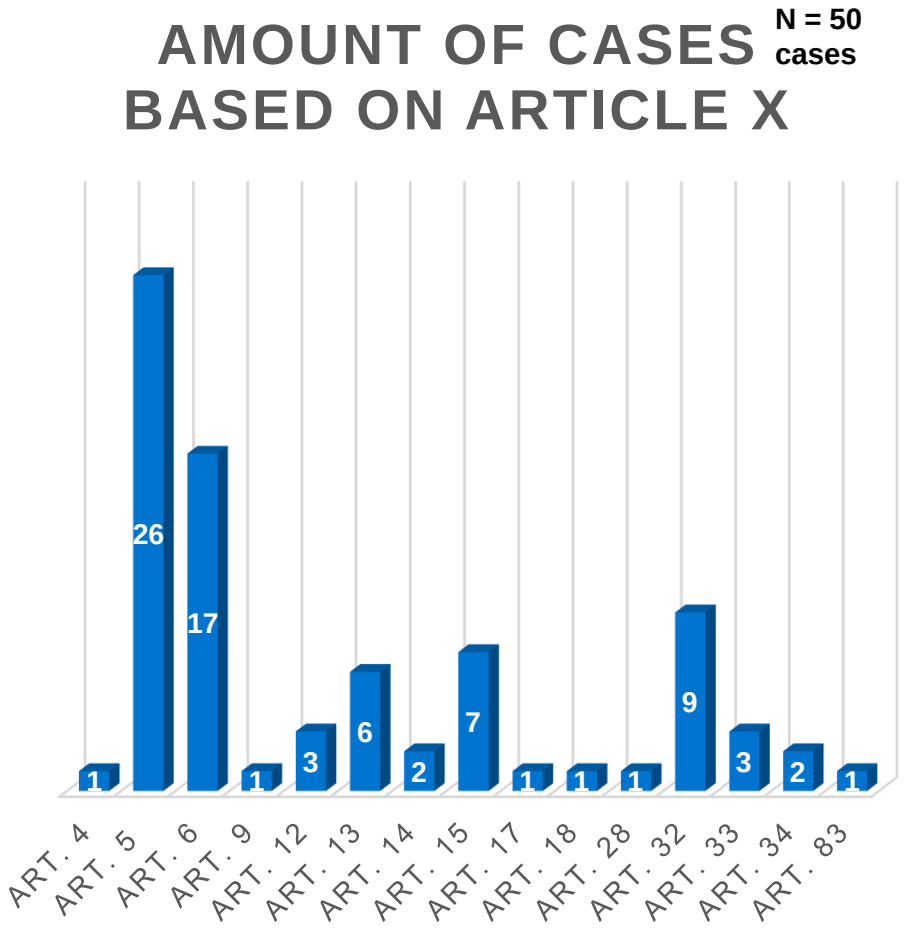

© sebis

# Approach – Activities derived from literature

- **Inform about regulation within organization** (e.g. introducing training programs for data controllers/processors)
- **Verify new and existing data handling processes regarding regulation compliance** (e.g. privacy by design and default, lawful basis of processing, data sharing)
- **Create data protection impact assessment (DPIA)**
- **Cooperation with supervisory authority**
- **Create records of Processing Activities**
- **Dealing with Data Subjects** (e.g. handle deletion/… requests, Inform about data use (e.g. privacy policy) and breaches)
- **Report to Management**


© sebis

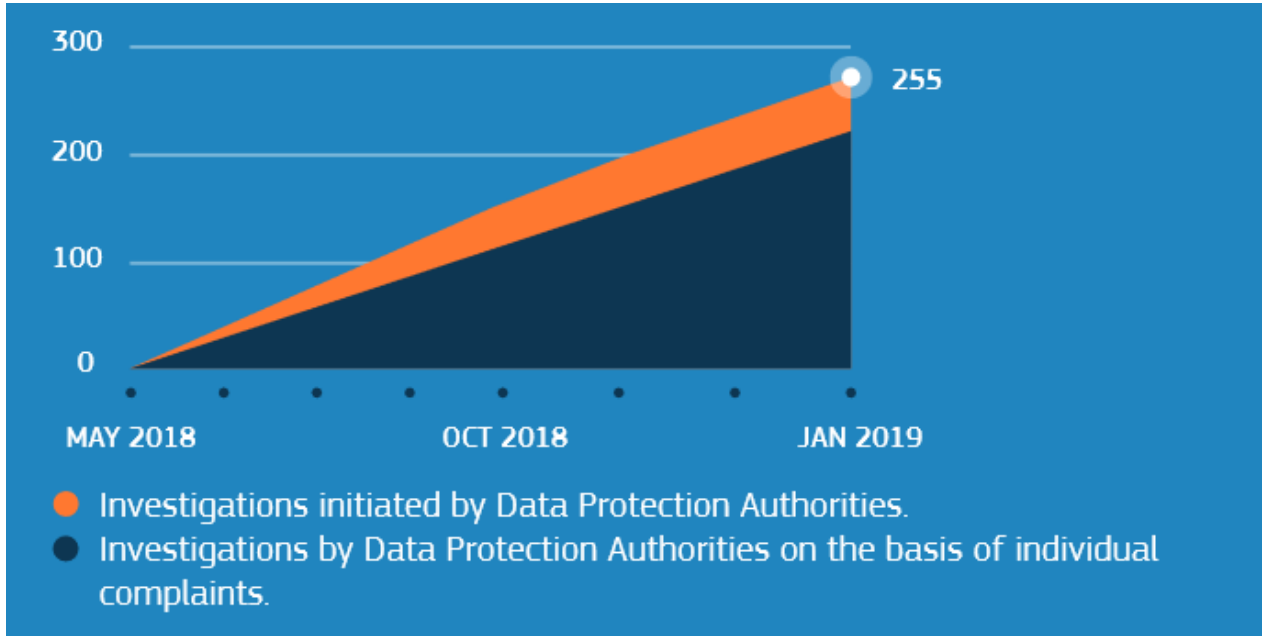
# Approach – Monetary value




http://www.enforcementtracker.com/

Official penalty sum in € [5]: ~ **56M**

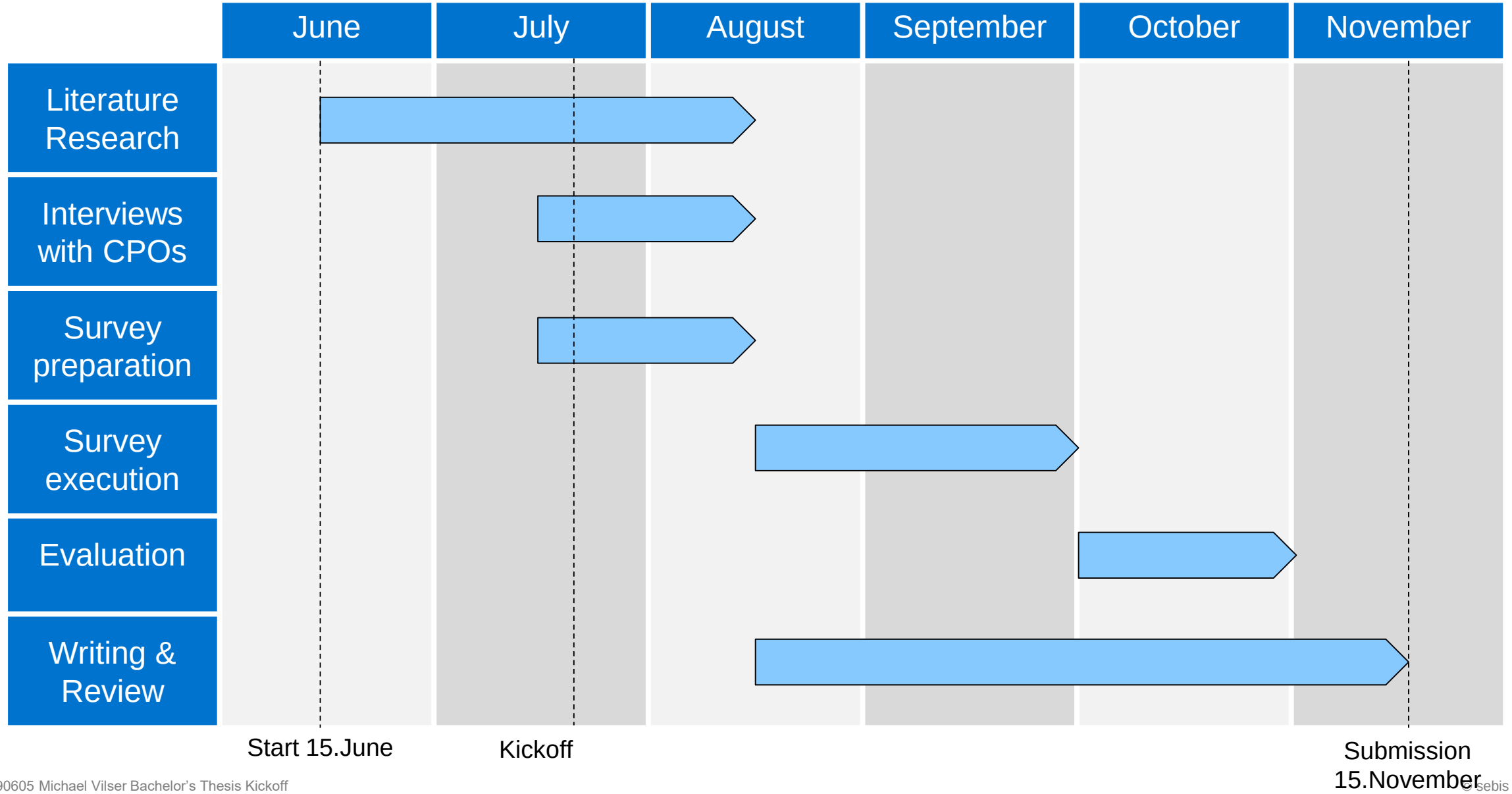
Penalty sum I calculated in €: ~ **52M**




[6]


© sebis

# Next Steps - Timetable



**Michael Vilser**

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

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289. 17132
Fax +49.89.289.17136

matthes@in.tum.de
wwwmatthes.in.tum.de

# References

[1] European Commission (2016), “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. 59, pp. 1-88.

[2] Huth, Dominik: Using Enterprise Architecture Models for Creating the Record of Processing Activities (Art. 30 GDPR).

[3] Burmeister, Fabian; Drews, Paul; Schirmer, Ingrid (2019): A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation. In : Proceedings of the 52nd Hawaii International Conference on System Sciences.

[4] Koç, Hasan; Eckert, Kai; Flaig, Daniel (2018): Datenschutzgrundverordnung (DSGVO): Bewältigung der Herausforderungen mit Unternehmensarchitekturmanagement (EAM). In *HMD Praxis der Wirtschaftsinformatik* 55 (5), pp. 942–963. DOI: 10.1365/s40702-018-00449-7.

[5] European Data Protection Board (2019): First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities. Available online at http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf, checked on 6/28/2019.


© sebis

# Backup
## RACI Matrix

| [1] [2] | DPO | Supervisory authority | Data Controllers | Data Processors | Management | Data Subject | How often? |
|---|---|---|---|---|---|---|---|
| **Inform about regulation within organization** (e.g. introducing training programs for data controllers/processors) | R | C | I | I | A, I | | Regularly |
| **Verify new and existing data handling processes regarding regulation compliance** (e.g. privacy by design and default, lawful basis of processing, data sharing) [4] | R | C | C, I | C, I | A | | Continuously |
| **Data protection impact assessment (DPIA)** | C | C, I | R (see Art. 35 II) | C | A, I | | "at least when there is a change of the risk represented by processing operations" Art 35 XI |
| **Cooperation with supervisory authority** | R | C | I | | A, I | | Continuously/On demand |
| **Records of Processing Activities** | (R,) C | I | R | R | A | | Continuously, inform SA on request |
| **Dealing with Data Subjects** (e.g. handle deletion/… requests, Inform about data use (e.g. privacy policy) and breaches) | C | | R | C | A | I | On request |
| **Report to Management** | R | | | | I | | On demand |


© sebis