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
www.matthes.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
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
Motivation

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

Enterprise Architecture Management

Data Protection Management

Enterprise Architect

Data Protection Officer
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?
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?
## Approach – Desired outcome

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

© sebris
**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
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**
Approach – Monetary value

AMOUNT OF CASES N = 50 cases
BASED ON ARTICLE X

Penalty sum I calculated in €: ~ 52M

Official penalty sum in € [5]: ~ 56M

http://www.enforcementtracker.com/

[6]

Investigations initiated by Data Protection Authorities.
Investigations by Data Protection Authorities on the basis of individual complaints.
Next Steps - Timetable

- **June**
  - Literature Research
  - Interviews with CPOs
  - Survey preparation
  - Evaluation
  - Writing & Review

- **July**
  - Literature Research
  - Interviews with CPOs
  - Evaluation

- **August**
  - Literature Research
  - Interview with CPOs
  - Survey preparation
  - Survey execution
  - Evaluation

- **September**
  - Literature Research
  - Survey execution
  - Evaluation

- **October**
  - Literature Research
  - Survey execution
  - Evaluation

- **November**
  - Literature Research
  - Survey execution

- **Start 15. June**
- **Kickoff**
- **Submission 15. November**
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
www.matthes.in.tum.de
References


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