Empirical Task Analysis of Data Protection Management

Bachelor's Thesis – Final Presentation
Michael Vilser 18.11.2019

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

1. Motivation
2. Approach
3. Activities
4. Survey Results
5. Conclusion
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 (Art. 83)
“Half of the survey respondents subject to GDPR state that they are far from compliance or will never comply”

- Annual Privacy Governance Report, 2018

What needs to be done to achieve compliance?

The GDPR specifies obligations but not their implementation.

How are these obligations met in practice?

What are the problems?

No detailed information about which and where problems occur.

If we don’t know the problems, we can’t mitigate them.

How can we mitigate these problems?

Guidelines? Tools? EAM support?

How effective is it?
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

Method

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

**Interviews with DPOs**
- Enhance domain knowledge
- Verify survey and list of activities

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

**Survey execution**
- Duration: 15.August to 4.October 2019
- 38 Participants

**Evaluation**
- Statistics
- Recommendations
1. **Awareness-raising and schooling within the organization concerning the GDPR:** e.g. by introducing training programs, newsletters

2. **Verify already existing data handling processes regarding compliance:** e.g. analyze which kind of data is used, for what purpose,…

3. **Creation of new data handling processes:** e.g. encourage privacy by design & default, discover possible violations in planned process and suggest alternatives,…

4. **Identify need & support creation of data protection impact assessments (DPIAs)**

5. **Cooperation with supervisory authority:** e.g. answer requests, notify about data breaches,…

6. **Create Records of Processing Activities (RPA):** contains contact details of responsible actor, purpose of processing,…

7. **Conducting Audits:** used to determine the organization’s current status regarding compliance

8. **Dealing with Data Subjects,** e.g. handle deletion/… requests, Inform about data use (e.g. privacy policy) and breaches

9. **Report to Management,** e.g. status reports of data protection management in general
## RACI Matrix

<table>
<thead>
<tr>
<th>Activities \ Stakeholders</th>
<th>DPO</th>
<th>Supervisory Authority</th>
<th>Data Controller</th>
<th>Data Processor</th>
<th>Management</th>
<th>Data Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness raising and schooling</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>A, I</td>
<td></td>
</tr>
<tr>
<td>Verify already existing data handling processes</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Creation of new data handling processes</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>A</td>
<td>I</td>
</tr>
<tr>
<td>Identify need &amp; conducting DPIAs</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>A, I</td>
<td></td>
</tr>
<tr>
<td>Cooperation with supervisory authority</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>A, I</td>
<td></td>
</tr>
<tr>
<td>Maintaining RPAs</td>
<td>C</td>
<td>I</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Conducting Audits</td>
<td>R</td>
<td></td>
<td>R</td>
<td>C</td>
<td>A, I</td>
<td></td>
</tr>
<tr>
<td>Dealing with Data Subjects</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td></td>
<td>A</td>
<td>I</td>
</tr>
<tr>
<td>Report to Management</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td>A, I</td>
<td></td>
</tr>
</tbody>
</table>

R = Responsible | A = Accountable | C = Consulted | I = Informed

Michael Vilser | Bachelor’s Thesis | Final Presentation

© sebis
Survey Results

General Information

38 DPOs from Germany

Educational Background (multiple answers were possible)

- 21 x IT
- 14 x Legal
- 14 x Economy
- 5 x Other

Work experience distribution (N=38)

Collaboration with EAM depending on organization size (N=38)
Survey Results
Complexity Distribution (N=38)

- Identify need & conducting DPIAs
- Verifying already existing data handling processes...
- Creation of new data handling processes
- Maintaining records of processing activities (RPAs)
- Dealing with Data Subjects
- Conducting Audits
- Awareness-raising and schooling within the...
- Report to Management
- Cooperation with supervisory authority

Survey Results
Complexity Distribution (N=38)

- Identify need & conducting DPIAs
- Verifying already existing data handling processes...
- Creation of new data handling processes
- Maintaining records of processing activities (RPAs)
- Dealing with Data Subjects
- Conducting Audits
- Awareness-raising and schooling within the...
- Report to Management
- Cooperation with supervisory authority

- Complexity = 1
- Complexity = 2
- Complexity = 3
- Complexity = 4
- Complexity = 5
Survey Results
Mean Time Consumption (N=38)

- Verifying already existing data handling... 20.41%
- Creation of new data handling processes 14.11%
- Awareness-raising and schooling within... 12.46%
- Maintaining records of processing... 12.46%
- Conducting Audits 11.08%
- Identify need & conducting DPIAs 10.30%
- Report to Management 7.11%
- Dealing with Data Subjects 7.00%
- Cooperation with supervisory authority 5.08%
Survey Results
Problem Frequencies (N=38)

“The Please select **two or less** most severe problems for each activity.”

<table>
<thead>
<tr>
<th>Activities/Problems</th>
<th>Legislation</th>
<th>Tools/Tech</th>
<th>Personnel</th>
<th>Guidelines</th>
<th>Contact persons</th>
<th>Authority</th>
<th>Holistic view</th>
<th>Single process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness-raising and schooling within the...</td>
<td>18%</td>
<td>16%</td>
<td>39%</td>
<td>26%</td>
<td>8%</td>
<td>13%</td>
<td>16%</td>
<td>16%</td>
</tr>
<tr>
<td>Verifying already existing data handling...</td>
<td>16%</td>
<td>18%</td>
<td>29%</td>
<td>26%</td>
<td>29%</td>
<td>11%</td>
<td>16%</td>
<td>24%</td>
</tr>
<tr>
<td>Creation of new data handling processes</td>
<td>16%</td>
<td>16%</td>
<td>29%</td>
<td>21%</td>
<td>24%</td>
<td>13%</td>
<td>13%</td>
<td>26%</td>
</tr>
<tr>
<td>Identify need &amp; conducting DPIAs</td>
<td>21%</td>
<td>21%</td>
<td>21%</td>
<td>29%</td>
<td>18%</td>
<td>5%</td>
<td>13%</td>
<td>21%</td>
</tr>
<tr>
<td>Cooperation with supervisory authority</td>
<td>5%</td>
<td>3%</td>
<td>21%</td>
<td>26%</td>
<td>18%</td>
<td>11%</td>
<td>5%</td>
<td>3%</td>
</tr>
<tr>
<td>Maintaining records of processing activities</td>
<td>11%</td>
<td>18%</td>
<td>18%</td>
<td>26%</td>
<td>11%</td>
<td>3%</td>
<td>21%</td>
<td>21%</td>
</tr>
<tr>
<td>Conducting Audits</td>
<td>11%</td>
<td>16%</td>
<td>24%</td>
<td>32%</td>
<td>11%</td>
<td>8%</td>
<td>13%</td>
<td>8%</td>
</tr>
<tr>
<td>Dealing with Data Subjects</td>
<td>21%</td>
<td>21%</td>
<td>8%</td>
<td>8%</td>
<td>8%</td>
<td>8%</td>
<td>8%</td>
<td>26%</td>
</tr>
<tr>
<td>Report to Management</td>
<td>8%</td>
<td>3%</td>
<td>16%</td>
<td>8%</td>
<td>8%</td>
<td>26%</td>
<td>5%</td>
<td>8%</td>
</tr>
</tbody>
</table>
Survey Results
Collaboration with EAM (N=12)

Effectiveness of EAM Support (N=12)

- Report to Management
- Verifying already existing data handling processes regarding compliance
- Creation of new data handling processes
- Maintaining records of processing activities (RPAs)
- Identify need & conducting DPIAs
- Awareness-raising and schooling within the organization
- Dealing with Data Subjects
- Conducting Audits
- Cooperation with supervisory authority
Survey Results
Reasons for missing Collaboration with EAM

Reasons for missing Collaboration with EAM (N=26)

EAM does not exist: 14
Don't know if EAM exist: 4
Missing contact persons: 4
No benefits: 2
EAM tools are hard to use: 2
No time on the part of EAM: 2
No time for my part: 2
Other goals/objectives/level of detail: 2
Other: 2
Conclusion

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

=> The identified Activities can be reliably used to cover tasks in DPM
=> Process-heavy Activities are especially complex and time consuming

RQ2) Which problems occur while performing these activities?

=> Lack of personnel and guidelines are problematic for many of these activities
=> Lack of information (sources) is especially severe for process-heavy activities

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

=> Collaboration rate: ~1/3
=> Collaboration with EAM proves beneficial for 8 of 9 activities
=> Non-existence of EAM in the organizations is the main reason for missing collaboration
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


AMOUNT OF CASES BASED ON ARTICLE X

N = 50 cases

Penalty sum I calculated in €: ~ 52M

Official penalty sum in € [5]: ~ 56M

[6]

http://www.enforcementtracker.com/