Certifications to Safeguard Data Protection Standards? How Superficial Internalization Thwarts the Plan

Philipp Danylak, Kathrin Brecker, Sebastian Lins, Ali Sunyaev
{philipp.danylak, kathrin.brecker, sebastian.lins, sunyaev}@kit.edu

Certifications’ Envisioned Potential
- Demonstrating compliance with data protection standards (EU-GDPR)
- Tackling current challenges in data governance
- Serving as a global mechanism for decentralized self-regulation through competitive pressure [1]
- Motivating companies to adopt data governance and protection standards [2–4]
- Reducing the asymmetric power distribution between individuals and companies by creating transparency about data processing practices [5]
- Enabling individuals to make better-informed decisions
- Providing guidance for organizations, clarifying requirements, and recommending best practices [6]

Certifications’ Envisioned Potential
- Demonstrating compliance with data protection standards (EU-GDPR)
- Tackling current challenges in data governance
- Serving as a global mechanism for decentralized self-regulation through competitive pressure [1]
- Motivating companies to adopt data governance and protection standards [2–4]
- Reducing the asymmetric power distribution between individuals and companies by creating transparency about data processing practices [5]
- Enabling individuals to make better-informed decisions
- Providing guidance for organizations, clarifying requirements, and recommending best practices [6]

Superficial Internalization Threat
- Policymakers demand rigorous internalization of the certification requirements [7,8]
- Internalization is defined as the process through which organizations incorporate certification information into their procedures and daily practices [9]
- Internalization includes explicit certification information (e.g., proposed data governance best practices)
- Internalization also includes tacit certification information (e.g., attestation results and feedback by auditors)
- Some organizations internalize certifications only at a superficial level, undermining their intended effects [10,11]
- Compliance is pretended but not achieved
- Superficial internalization threatens the effectiveness of certifications as a mechanism for data governance

Research Question
What are potential pitfalls and which measures for mitigation can be taken in order to leverage data protection certifications to safeguard the requirements of the GDPR? (Descriptive Literature Review [13])

Don’t (Pitfalls) Do (Mitigation)

<table>
<thead>
<tr>
<th>No.</th>
<th>Pitfall Description</th>
<th>Mitigation Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Adopt data protection certifications solely motivated by external pressure [14-16] (e.g., customer demands, government regulations)</td>
<td>Approach data protection certifications as an opportunity for internal improvement and legal requirements’ clarification [16-18]</td>
</tr>
<tr>
<td>2</td>
<td>Adopt data protection certifications with a lack of stakeholder engagement [19-23] (e.g., executive buy-in, employee involvement)</td>
<td>Internalize data protection certifications with a focus on stakeholder communication, executive buy-in, and employee participation [22,24,25]</td>
</tr>
<tr>
<td>3</td>
<td>Adopt data protection certifications following a sole top-down (based on defined to-be state) [21,22] or bottom-up (based on current as-is state) approach [19,26]</td>
<td>Implement data protection certifications following a discursive approach for improvements while considering the as-is state [19-22]</td>
</tr>
</tbody>
</table>

Conclusion
Certifications can only contribute to the safeguarding of data protection standards when risks of superficial internalization are mitigated and pitfalls avoided.
CERTIFICATIONS TO SAFEGUARD DATA PROTECTION STANDARDS?  
HOW SUPERFICIAL INTERNALIZATION THWARTS THE PLAN

Philipp Danylak, Kathrin Brecker, Sebastian Lins, Ali Sunyaev
{philipp.danylak, kathrin.brecker, sebastian.lins, sunyaev}@kit.edu

References


