

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]

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)
1	Adopt data protection certifications solely motivated by external pressure [14-16] (e.g., customer demands, government regulations)	Approach data protection certifications as an opportunity for internal improvement and legal requirements' clarification [16-18]
2	Adopt data protection certifications with a lack of stakeholder engagement [19-23] (e.g., executive buy-in, employee involvement)	Internalize data protection certifications with a focus on stakeholder communication, executive buy-in, and employee participation [22,24,25]
3	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]	Implement data protection certifications following a discursive approach for improvements while considering the as-is state [19-22]

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

- [1] A. A. King, M. J. Lenox, and A. Terlaak, "The Strategic Use of Decentralized Institutions: Exploring Certification With the ISO 14001 Management Standard," *Academy of Management Journal*, vol. 48, no. 6, pp. 1091–1106, 2005, doi: 10.5465/amj.2005.19573111.
- [2] I. Guler, M. F. Guillén, and J. M. Macpherson, "Global Competition, Institutions, and the Diffusion of Organizational Practices: The International Spread of ISO 9000 Quality Certificates," *Administrative Science Quarterly*, vol. 47, no. 2, pp. 207–232, 2002, doi: 10.2307/3094804.
- [3] P. Christmann and G. Taylor, "Firm self-regulation through international certifiable standards: determinants of symbolic versus substantive implementation," *Journal of International Business Studies*, vol. 37, no. 6, pp. 863–878, 2006, doi: 10.1057/palgrave.jibs.8400231.
- [4] P. Christmann and G. Taylor, "Globalization and the Environment: Determinants of Firm Self-Regulation in China," *Journal of International Business Studies*, vol. 32, no. 3, pp. 439–458, 2001, doi: 10.1057/palgrave.jibs.8490976.
- [5] J. Löbbers, S. Lins, T. Kromat, A. Benlian, and A. Sunyaev, "A multi-perspective lens on web assurance seals: contrasting vendors' intended and consumers' perceived effects," *Electronic Commerce Research*, pp. 1–43, 2020, doi: 10.1007/s10660-020-09415-2.
- [6] N. Maier, S. Lins, H. Teigeler, A. Roßnagel, and A. Sunyaev, "Die Zertifizierung von Cloud-Diensten nach der DSGVO," *Datenschutz Datensich*, vol. 43, no. 4, pp. 225–229, 2019, doi: 10.1007/s11623-019-1097-3.
- [7] J. A. Briscoe, S. E. Fawcett, and R. H. Todd, "The Implementation and Impact of ISO 9000 among Small Manufacturing Enterprises," *Journal of Small Business Management*, vol. 43, no. 3, pp. 309–330, 2005, doi: 10.1111/j.1540-627X.2005.00139.x.
- [8] E. Naveh and A. A. Marcus, "When does the ISO 9000 quality assurance standard lead to performance improvement? Assimilation and going beyond," *IEEE Transactions on Engineering Management*, vol. 51, no. 3, pp. 352–363, 2004, doi: 10.1109/TEM.2004.830864.
- [9] G. A. Knight and P. W. Liesch, "Information internalisation in internationalising the firm," *Journal of Business Research*, vol. 55, no. 12, pp. 981–995, 2002, doi: 10.1016/s0148-2963(02)00375-2.
- [10] P. Stephanow and C. Banse, "Evaluating the Performance of Continuous Test-Based Cloud Service Certification," in *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, 2017, pp. 1117–1126.
- [11] O. Boiral, "ISO 9000: Outside the Iron Cage," *Organization Science*, vol. 14, no. 6, pp. 720–737, 2003, doi: 10.1287/orsc.14.6.720.24873.
- [12] I. Heras-Saizarbitoria, O. Boiral, and A. Díaz de Junguitu, "Environmental management certification and environmental performance: Greening or greenwashing?," *Business Strategy and the Environment*, vol. 29, no. 6, pp. 2829–2841, 2020, doi: 10.1002/bse.2546.
- [13] G. Paré, M.-C. Trudel, M. Jaana, and S. Kitsiou, "Synthesizing information systems knowledge: A typology of literature reviews," *Information & Management*, vol. 52, no. 2, pp. 183–199, 2015, doi: 10.1016/j.im.2014.08.008.
- [14] D. I. Prajogo, "The roles of firms' motives in affecting the outcomes of ISO 9000 adoption," *International Journal of Operations & Production Management*, vol. 31, no. 1, pp. 78–100, 2011, doi: 10.1108/01443571111098753.
- [15] J. J. Tarí, J. Pereira-Moliner, J. F. Molina-Azorín, and M. D. López-Gamero, "Heterogeneous adoption of quality standards in the hotel industry: drivers and effects," *International Journal of Contemporary Hospitality Management*, vol. 31, no. 3, pp. 1122–1140, 2019, doi: 10.1108/IJCHM-09-2017-0606.
- [16] S. Lins, T. Kromat, J. Löbbers, A. Benlian, and A. Sunyaev, "Why Don't You Join In? A Typology of Information System Certification Adopters," *Decision Sciences*, pp. 1–34, 2020, doi: 10.1111/dec.12488.
- [17] C. Valmohammadi and M. Kalantari, "Using structural equation modelling to test ISO 9000 motivation, depth of ISO implementation and performance of Iranian manufacturing organisations," *International Journal of Productivity and Quality Management*, vol. 20, no. 3, pp. 405–427, 2017, doi: 10.1504/IJPQM.2017.082675.
- [18] A. Nair and D. Prajogo, "Internalisation of ISO 9000 standards: the antecedent role of functionalist and institutional drivers and performance implications," *International Journal of Production Research*, vol. 47, no. 16, pp. 4545–4568, 2009, doi: 10.1080/00207540701871069.
- [19] O. Boiral, "Corporate Greening Through ISO 14001: A Rational Myth?," *Organization Science*, vol. 18, no. 1, pp. 127–146, 2007, doi: 10.1287/orsc.1060.0224.
- [20] H. Yin and P. J. Schmeidler, "Why do standardized ISO 14001 environmental management systems lead to heterogeneous environmental outcomes?," *Business Strategy and the Environment*, vol. 18, no. 7, pp. 469–486, 2009, doi: 10.1002/bse.629.
- [21] G. Guzman and L. F. Trivelato, "Transferring codified knowledge: socio-technical versus top-down approaches," *Learning Organization*, vol. 15, no. 3, pp. 251–276, 2008, doi: 10.1108/09696470810868873.
- [22] K. W. Sandholtz, "Making Standards Stick: A Theory of Coupled vs. Decoupled Compliance," *Organization Studies*, vol. 33, 5/6, pp. 655–679, 2012, doi: 10.1177/0170840612443623.
- [23] C. W. Hsu, "Frame misalignment: interpreting the implementation of information systems security certification in an organization," *European Journal of Information Systems*, vol. 18, no. 2, pp. 140–150, 2009, doi: 10.1057/ejis.2009.7.
- [24] O. Boiral, I. Heras-Saizarbitoria, and M.-C. Brotherton, "Corporate Biodiversity Management through Certifiable Standards," *Business Strategy and the Environment*, vol. 27, no. 3, pp. 389–402, 2018, doi: 10.1002/bse.2005.
- [25] I. Heras-Saizarbitoria and O. Boiral, "Symbolic adoption of ISO 9000 in small and medium-sized enterprises: The role of internal contingencies," *International Small Business Journal*, vol. 33, no. 3, pp. 299–320, 2015, doi: 10.1177/0266242613495748.
- [26] V. S. Amundsen and T. C. Osmundsen, "Becoming certified, becoming sustainable? Improvements from aquaculture certification schemes as experienced by those certified," *Marine Policy*, vol. 119, pp. 1–8, 2020, doi: 10.1016/j.marpol.2020.104097.