On the Evaluation of Privacy Impact Assessment and Privacy Risk Assessment Methodologies: A Systematic Literature Review

Wairimu, S (Karlstads Universitet)., Iwaya, L.H.(Karlstads Universitet), Fritsch, L.(OsloMet) and Lindskog, S (Karlstads Universitet)

Assessing privacy risks and incorporating privacy measures from the onset requires a comprehensive understanding of potential impacts on data subjects. Privacy Impact Assessments (PIAs) offer a systematic methodology for such purposes, which are closely related to Data Protection Impact Assessments (DPIAs), particularly outlined in Article 35 of the General Data Protection Regulation (GDPR). The core of a PIA is a Privacy Risk Assessment (PRA). PRAs can be integrated as part of full-fledged PIAs or independently developed to support PIA processes. Although these methodologies have been identified as essential enablers of privacy by design, their effectiveness has been criticized because of the lack of evidence of their rigorous and systematic evaluation. Hence, we conducted a Systematic Literature Review (SLR) to identify published PIA and PRA methodologies and assess how and to what extent they have been scientifically validated or evaluated. We found that these methodologies are rarely evaluated for their performance in practice, and most of them have only been validated in limited studies. Most validation evidence is found with PRA methodologies. Of the evaluated methodologies, PIAs were the most evaluated, where case studies were the predominant evaluation method. These evaluated methodologies can be easily transferred to an industrial setting or used by practitioners, as they provide evidence of their use in practice. In addition, the findings in this study can be used to inform researchers of the current state-of-the-art, and practitioners can understand the benefits and current limitations of the methodologies and adopt evidence-based practices.