ABSTRACT

The advancement of information and communication technology (ICT) in the digital era has driven rapid growth in the use and dissemination of personal data across various digital platforms by individuals, significantly increasing the risk of privacy breaches during personal data processing. These challenges have become increasingly critical for both individuals and organizations in ensuring the management of personal data aligns with data protection principles. Although the Indonesian government has enacted Law No. 27 of 2022 on Personal Data Protection, the optimal implementation of this regulation faces significant obstacles. One notable challenge is the absence of derivative regulations providing detailed and technical guidance for conducting personal data protection impact assessments. This gap has resulted in organizations struggling to identify and manage privacy risks associated with personal data processing. This study aims to develop a risk-based personal data protection impact assessment instrument. Employing a qualitative methodology with a Grounded Theory approach, the study designed an instrument that comprises eight personal data protection principles and 37 assessment components for evaluating data protection practices. The assessment results were analyzed using the ISO 27005:2018 risk management framework, applying a three-dimensional matrix consisting of asset security value, breach actions, and principles violations to determine the impact level of each identified risk. Instrument was implemented at a cybersecurity consultancy, leading to the identification of 47 high-impact risks. These findings serve as the foundation for formulating strategic recommendations, focusing on mitigating high-impact risks to enhance personal data protection within organizations. This research makes a practical contribution by developing an instrument that effectively aids organizations in identifying, analyzing, and managing privacy risks related to personal data management. Additionally, the instrument holds potential as a practical reference for organizations to meet the requirements of personal data protection laws and improve compliance with personal data protection principles.

Keywords *– Data Privacy, Data Security, Personal Data Protection Impact Assessment, Privacy Risk, Personal Data Protection*