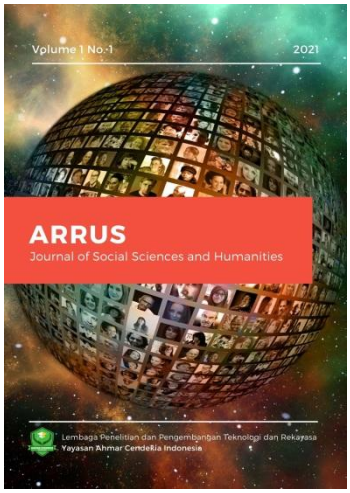
https://doi.org/10.35877/soshum5132

OPEN ACCESS

ISSN: 2776-7930 (Print) / 2807-3010 (Online)



RESEARCH ARTICLE

Understanding Privacy Policy Compliance in Digital SMEs: The Role of TOE Factors, Compliance Readiness, and BPM Capability

Putri Pradnyawidya Sari[1*], Munir Munir[1], Chairul Furqon[1], Asep Wahyudin[1], & Erwin Sutomo[2]

[1] Department of Management, Faculty of Economics and Business, Universitas Pendidikan Indonesia, Bandung, Indonesia.
[2] Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, Pahang, Malaysia.

*Corresponding author: Putri Pradnyawidya Sari, Department of Management, Faculty of Economics and Business, Universitas Pendidikan Indonesia, Bandung, Indonesia

E-mail: putripradnya@upi.edu

Abstract: Today, more and more digital SMEs utilize various online tools such as social media, marketplaces, online payment methods, etc., to collect data about customers; yet, often privacy compliance is done in an informal manner and is not always integrated into company routines. The current research explores how technological, organizational and environmental factors affect privacy policy compliance via compliance readiness and Business Process Management (BPM) capability. The uniqueness of the research is in the use of the Technology-Organization-Environment (TOE) framework, organizational readiness and BPM capability in the context of sequential mediation. The study used the quantitative cross-sectional survey which was conducted among 174 owners, managers, and employees of Indonesian digital SMEs selected by means of purposive sampling. The analysis of the gathered data was carried out using Partial Least Squares Structural Equation Modeling (PLS-SEM) in SmartPLS with such steps as the evaluation of measurement model, bootstrapping with 5,000 resamples, and testing of predictive relevance. It has been found that TOE factors greatly influence the level of compliance readiness and even increase BPM capability. Organizational readiness positively affects BPM capability and privacy policy compliance whereas BPM capability influences privacy policy compliance too. 54.9% of the variance in privacy policy compliance can be explained by the model. All indirect effects via compliance readiness, BPM capability, and the sequence of these factors have proven to be significant. This means that positive technology, organizational support, and environmental pressure do not guarantee compliance practices. Firstly, digital SMEs need to develop their internal readiness and then implement it in terms of documented, monitored and repeatable business processes.

Keywords: TOE Framework, Compliance Reeadiness, BPM Capability, Privacy Policy Compliance, Digital SMEs

1. Introduction

The use of digital transformation has transformed the way of working for SMEs in Indonesia. More and more SMEs have been using electronic commerce, social media, cloud computing applications, and digital payments to connect with consumers and make deals with them. With the spread of digital technology, the process of managing personal data no longer applies just to big companies but also to smaller companies operating on digital platforms.

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Thus, phone numbers, addresses, transaction records, and identification details of consumers have become part of the routine work of SMEs, which brings new privacy and security issues.

Within the past few years, the government in Indonesia has strengthened the regulation of data protection through the introduction of national legislation concerning personal data. The regulations require organizations to guarantee proper data collection, processing, storage, and utilization. Despite the widespread applicability of this regulation framework in several industries, the implementation of this framework within micro, small, and medium enterprises (MSMEs) is inconsistent. In reality, many digital MSMEs emphasize operational consistency, income generation, and expansion into new markets, while their focus on privacy compliance within their management is usually inadequate. The reasons for this are resource constraints, lack of organizational procedures, and lack of knowledge in managing operations.

Privacy protection, cybersecurity, and compliance issues have been studied in terms of organizations' (Kshetri, 2017; Martin et al., 2017). . Moreover, the TOE model has been used in order to consider the impact of the technology and environment on organizational decision-making and activities (Gangwar et al., 2015b; Oliveira & Martins, 2011). The main idea of the TOE model is that technological readiness, organizational support, and environmental factors influence organizational strategy and activities. However, the literature review shows that there is a supposition about direct connection between the factors and compliance issues. It does not take into account the SME context in which different organizations have different readiness and skills.

External pressure by itself is not enough in many micro, small, and medium-sized enterprises (MSMEs) to make the organizations adopt the practices of sustainable compliance. Although organizations understand the significance of protecting personal information, they still face problems implementing proper processes and maintaining proper controls. This means that, apart from the influences coming from the outside, there are internal factors that affect compliance. Therefore, this paper highlights the role of compliance readiness as one of the important elements in explaining the ability of MSMEs to implement privacy policies. As it follows from the theory of organizational readiness (Weiner, 2009), compliance readiness includes an organization's willingness, awareness, and readiness to respond to regulations.

The current study proposes that privacy compliance for MSMEs is inextricably linked with the capability to perform key business processes. In a digitalized business landscape, privacy protection must be incorporated into business operations, such as customer registration, transaction processing, data storage, and data access. MSMEs with higher levels of Business Process Management (BPM) capabilities are likely to be more efficient in developing formal practices, monitoring data activities, and consistently implementing privacy controls. Literature suggests that BPM capabilities affect organizational efficiency and process standardization under changing business circumstances (Dumas et al., 2018; Schmiedel, Recker, & Vom Brocke, 2020). However, studies investigating the contribution of BPM to privacy policy compliance are scant.

Based on existing issues, this study formulates a comprehensive framework by integrating various TOE factors, compliance readiness, BPM capabilities, and compliance with privacy policies. In contrast to previous studies which focused on the direct relationship between contextual factors and compliance outcomes, this study places emphasis on the internal processes through which compliance is implemented in SMEs. The proposed model makes compliance readiness and BPM capabilities a connecting tool that links organizational context with actual compliance practices.

This study contributes to the literature in several aspects. First, this study enriches the TOE framework by adding compliance readiness and BPM capabilities in an integrated model for basic privacy compliance. Second, this study provides empirical evidence from the context of digital SMEs in Indonesia, which is still under-examined in investigations related to privacy compliance. Third, this study provides a strategic view for SME owners and policy makers regarding the importance of organizational readiness and process capabilities in establishing

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

sustainable privacy management. With a quantitative approach taken from reviewing data on digital SMEs, this study empirically examines the relationships between proposed constructs and provides a deeper understanding of how SMEs can improve privacy compliance in the digital economy.

2. Literature Review

2.1. Privacy Policy Compliance in Digital SMEs

Compliance with privacy regulations is now a concern in information management and systems, as digital businesses increasingly rely on the collection and use of personal data. Previous research on information privacy emphasizes that privacy concerns not only individuals but also organizations, as companies are responsible for designing, managing, and communicating data processing practices to customers, employees, and partners (Belanger & Crossler, 2011; Smith et al., 2011). As far as the world of online commerce is concerned, the expectation is that the privacy policies, consent procedures, and data handling will lessen uncertainties and encourage trust. According to Milne and Culnan (2004), privacy disclosures have an important role in addressing online privacy concerns, although it is a fact that a large number of users do not read or understand them completely(Milne & Culnan, 2004). This indicates that adherence to privacy laws must not be taken only in terms of having the policies. Instead, there should be established procedures for their implementation.

The importance of privacy compliance for management may be seen from two different angles - one of the customers' behaviors, and another of the performance of companies. Martin et al. (2017) assert that any fragility in customer information can have a detrimental effect on customers' trust and company performance, while transparency and control of customers can reduce the negative impact of the misuse of the data (Martin et al., 2017a). For small and medium-sized companies operating on the digital market, it is particularly important because their customers' interactions with the company occur through multiple purchases made through online platforms and social networks. The management of addresses, mobile phones, purchasing history, and other customer data becomes part of business processes.

On a regulatory perspective, based on the studies conducted on data protection, it is clear that in order to comply with the law, changes have to be done in terms of data management in the organizations. According to Tikkinen Piri et al., (2018), data protection laws have a direct impact on how firms manage their personal data in terms of collecting, processing and using it. Furthermore, according to Labadie & Legner (2023), in order for an organization to continue to remain in compliance with data protection, the organization should have its data management capabilities in place.

The MSME context entails specific problems. Small firms often face difficulties associated with a lack of finance, formal mechanisms, and poor cybersecurity knowledge. From this, it is clear that the use of cyber awareness and educational techniques specifically for micro-firms needs to be more precise since traditional security approaches do not always fit the size of those companies (Bada & Nurse, 2019). Thus, the statement that MSMEs operating online need a compliance model taking into account the peculiarities of operation seems to be true. In the current study, compliance with privacy laws will be defined as the implementation of privacy policies by MSMEs.

Technology, Organization, and Environment Factors as Contextual Drivers

The Technology-Organization-Environment (TOE) approach is extensively applied to explain how technology is adopted and implemented in organizations or business environments. In TOE-related research, the technological aspect reflects the technology's readiness, suitability, and ease of use. The organizational aspect is related to managerial support, human resources, and organizational capacity. The environmental aspect is influenced by competition in the market, regulations, partners' requirements, and customers' demands. The TOE conceptual framework is applied as an analytical tool to understand the

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

mechanisms of electronic system adoption in a corporate context. This framework reveals that the technology adoption process at the organizational level is influenced by three main categories of factors: the level of technology readiness, the structural and cultural characteristics of the organization, and the external environmental conditions surrounding business activities (Zhu et al., 2003). Later studies confirm that TOE is useful for explaining cloud computing, enterprise systems, and digital commerce adoption in organizations and SMEs (Awa et al., 2015; Gangwar et al., 2015a; Low et al., 2011; Ramdani et al., 2009).

In the context of data privacy policy compliance, the TOE (technology, organization, environment) theoretical framework offers an adequate contextual foundation for analyzing the phenomenon of technology adoption in the small and medium-sized business sector. Technological factors are highly significant because small and medium-sized businesses require an adequate digital infrastructure foundation, a strict access control system, secure data storage mechanisms, and monitoring tools to effectively manage personal information. The organizational variables play a crucial role in terms of commitment of management towards compliance, awareness about data protection on part of employees, allocation of duties in an organized manner and the availability of required resources, all of which are important aspects of designing a privacy policy framework. Environmental variables are of equal importance as well due to the reasons such as expectations of regulatory bodies, customer trust about handling data, market requirements, and risk of reputation damage, which create external pressure for small and medium sized enterprises to strengthen their personal data protection efforts. The above stated logic is consistent with the conclusions drawn through TOE approach based studies, according to which organizational behavior stems from the interaction of technology, organization and environment (Gangwar et al., 2015a; Low et al., 2011).

However, there is no denying that the use of the TOE framework in a direct way has certain limitations. Many researchers who have used the TOE framework focus mainly on the adoption decision-making process or on attaining the results from technology implementation. However, in the context of compliance with personal data protection policy, one basic difference exists: the idea of compliance cannot be reduced just to the adoption of technology but means some continuous processes within organizations which require such elements as commitment, interpretation, monitoring, and control. As Ramdani et al. (2009) found out, the adoption of enterprise information system varied greatly across small and medium-sized enterprises even when they had quite similar competitive conditions(Ramdani et al., 2009). This indicates that only contextual conditions cannot explain why some SMEs are more likely to comply than others. Therefore, the TOE framework serves as a contextual antecedent while the Compliance Readiness Contract and Business Process Management Capability become internal mechanisms through which contextual conditions are transformed into compliance practices.

Within the context of the TOE framework, the technological, organizational, and environmental aspects are expected to influence how prepared digital SMEs are to comply with privacy policies. The technological aspect provides the means for securing the information, the organizational aspect captures the managerial commitment and internal resources, while the environmental aspect imposes the external pressures through regulations, customer demands, and reputation issues. If these contextual aspects are favorable, then the SMEs will be capable of being aware, committed, and able to meet the privacy policies. Therefore, the following hypothesis can be proposed:

H1: TOE factors positively influence compliance readiness.

The TOE factors could possibly have an effect on BPM capability development. Technology helps organizations record and track processes related to data, and organization gives the resources required for process formalization. In addition, external pressure makes companies make things standardized in their organizations. The existing literature on TOE suggests that the context has an effect on how organizational adoption and implementation takes place

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

(Gangwar et al., 2015a; Low et al., 2011; Zhu et al., 2003). When it comes to privacy regulation, such context factors would make SMEs improve their process capability. Hence, the hypothesis is the following:

H2: TOE factors positively influence BPM capability.

2.2. *Compliance Readiness as an Internal Preparedness Mechanism*

The concept of compliance readiness used in the current research stems from the wider notion of organizational readiness for change. According to the literature, organizational readiness for change is the shared psychological condition of organizations that consists of two basic elements: commitment to change and change efficacy (Weiner, 2009). The former refers to the willingness of organization members to implement the desired change, while the latter refers to their belief in the ability of the organization to implement the change successfully. This conceptualization is particularly relevant in the context of data privacy compliance because it is applicable to the challenges faced by small and medium-sized businesses (SMEs) who might realize the significance of such legislation yet be unable to implement it due to some barriers.

The literature on organizational readiness suggests that the success of the implementation process depends on how change is perceived by organizational members, the availability of resources, and the expectations of consequences of such changes. An instrument for measuring organizational readiness for change includes change appropriateness, management support, change efficacy, and personal valence (Holt et al., 2007). Organizational readiness is viewed as a multilevel construct which ties the antecedents of implementation and the results of the implementation process (Rafferty et al., 2013). The construct of organizational readiness for implementing change was found to be a valid construct based on the theory of organizational readiness for change (Shea et al., 2014; Weiner, 2009). The combination of these sources gives grounds to assume that the construct of organizational readiness for implementing change is empirically testable.

In relation to digital transformation, the concept of organizational readiness has become more apparent. Organizational readiness for digital innovation refers to a multidimensional concept composed of four main components: resource readiness, IT readiness, cognitive readiness, and partnership readiness (Lokuge et al., 2019). The framework becomes highly pertinent when we consider the digital age and the context of small and medium-sized enterprises (SMEs), where personal data protection compliance requires the right digital competencies as well as organizational readiness. It is not enough for SMEs just to have the tools. They also need to understand how these tools impact personal data protection compliance.

Various studies conducted concerning compliance in the field of information systems have revealed that certain critical determinants play a crucial role in defining compliance behavior, such as awareness, belief, perceived effectiveness, and routine. Research shows that information security awareness and rational beliefs play a significant role in determining intentions to comply with information security policies (Bulgurcu et al., 2010). Protection and prevention motivations are identified as highly relevant factors in regard to information security policy compliance (Herath & Rao, 2009). Combining Protection Motivation Theory with the Theory of Planned Behavior provides a strong foundation for understanding information systems security policy compliance (Ifinedo, 2012). Compliance can be best obtained through fostering necessary awareness, beliefs, routines, and skills, with routines acting as reinforcing factors for compliant behavior (Vance et al., 2012). In this particular research study, compliance readiness represents these factors inside an organization.

Readiness for compliance means the extent to which SMEs are aware of, committed to, and able to meet the privacy-related requirements. Those firms that show high readiness will be in a better position to translate regulatory expectations into concrete action within their organizations. According to literature dealing with readiness for change, readiness depends

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

on such factors as commitment, self-efficacy, appropriateness perception, and management support (Holt et al., 2007; Shea et al., 2014; Weiner, 2009). The following hypothesis is put forward in the current research based on the idea that compliance readiness will motivate SMEs to build up formal business practices concerning personal information management:

H3: Compliance readiness positively influences BPM capability.

Compliance readiness is also said to have an impact on privacy policy compliance. SMEs that understand their privacy responsibilities and have organizational commitment will be better able to adhere to their privacy policies in their daily business processes. Research conducted regarding information security compliance reveals that awareness, perception of efficacy, and organizational beliefs can lead to compliance (Bulgurcu et al., 2010; Herath & Rao, 2009; Ifinedo, 2012). Thus, the higher compliance readiness of SMEs would result in higher privacy policy compliance. Hence, the following hypothesis is put forth:

H4: Compliance readiness positively influences privacy policy compliance.

2.3. BPM Capability as an Operational Mechanism for Privacy Compliance

BPM capabilities are very vital in ensuring data privacy compliance because privacy needs to be practiced in the normal operations of an organization. In the case of small and medium-sized organizations that rely on the use of digital technologies, personal data is processed during a number of operational stages, such as customer registration, orders handling, payments validation, delivery of products, consumer complaints handling, promotions, and post-purchase communication. It becomes hard to meet the desired level of data privacy compliance when all these stages are performed in an informal and undocumented manner.

A literature review on Business Process Management shows that process capabilities contribute to organizational effectiveness when aligned with the organization's context. Trkman (2010) argues that successful BPM implementation requires alignment between business processes and the business environment, accompanied by continuous development and adequate organizational support. Organizations can use Business Process Management (BPM) maturity models to assess, understand, and systematically enhance their process capabilities (Roglinger et al., 2012). Effective BPM implementation requires consideration of the specific organizational context, since a universal best-practice approach may not be appropriate across different organizational settings (vom Brocke et al., 2016). This aspect is particularly significant for small and medium-sized enterprises (SMEs), given that they relatively rarely have similar process structures, resources, and governance systems as larger enterprises.

Empirical studies on Business Process Management also reveal the crucial role of organizational culture and work methods in BPM implementation. Effective BPM implementation and improved process performance are influenced by an organizational culture that supports BPM practices and methods (Schmiedel et al., 2014; Schmiedel, Recker, & vom Brocke, 2020). Regarding the compliance of data privacy regulations, it can be observed that the formal approach, consisting of documentation, control points, process monitoring, and corrections, tends to be more efficient in the presence of a corporate culture focused on business process compliance.

In connection with the relation between BPM and personal data protection, there are findings related to data management capabilities. Successful implementation of compliance with personal data protection regulations requires the emergence of certain data management capabilities in organizations (Labadie & Legner, 2023). According to the authors' findings, such compliance should be based on three major components: organizational structure, management skills, and relationships with the environment. It can be argued that such findings support the theories stating that compliance with data privacy policies has to be ensured through a set of business processes. In this paper, BPM capability construct serves as the operational link between the concept of compliance readiness and adherence to data privacy policies.

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

The ability of BPM refers to the operational capability by which privacy policies can be incorporated into the day-to-day operations of an organization. In small- and medium-sized enterprises (SMEs) utilizing digital technology, personal data will be processed by way of routine actions such as registering customers, managing transactions, verifying payments, data storage, and customer communications. Through the documentation, standardization, monitoring, and continuous improvement of these processes, SMEs will have greater potential for incorporating their privacy controls consistently. BPM studies have shown that process capability influences organizational performance and process performance (Roglinger et al., 2012; Schmiedel, Recker, & vom Brocke, 2020; Trkman, 2010). Therefore, BPM capability is expected to contribute to the implementation of privacy policies. The following hypothesis is made:

H5: BPM capability positively influences privacy policy compliance.

2.4. Mediating Roles of Compliance Readiness and BPM Capability

The literature review provides an important foundation, but several knowledge gaps remain that require further attention. First, research on privacy has largely examined issues of privacy, consumer trust, customer vulnerability, and information security compliance, while only a limited number of studies have specifically examined privacy policy compliance as an organizational capability in digital-based small and medium enterprises (Belanger & Crossler, 2011; Martin et al., 2017b; Smith et al., 2011). Second, studies based on the TOE framework have successfully explained the phenomenon of digital technology adoption and enterprise information system implementation, but often focus on contextual drivers and pay relatively little attention to the internal mechanisms responsible for transforming the external context into sustainable compliance behavior (Gangwar et al., 2015a; Ramdani et al., 2009; Zhu et al., 2003). Third, research on organizational readiness provides a comprehensive explanation of implementation readiness, but the construct is rarely directly linked to privacy policy compliance in the context of small and medium-sized enterprises (SMEs) (Lokuge et al., 2019; Shea et al., 2014; Weiner, 2009). Fourth, research on Business Process Management shows the importance of process capabilities and process culture in organizations, but the role of these constructs in the context of privacy compliance in digital-based small and medium enterprises is still relatively underdeveloped (Labadie & Legner, 2023; Schmiedel et al., 2014; Trkman, 2010).

The novelty of this study lies in the integration of the previously outlined conceptual streams. Rather than treating the TOE framework factors as direct predictors of privacy compliance, this study positions the constructs of compliance readiness and Business Process Management capabilities as mediating mechanisms linking contextual factors to compliance behavior. These constructs have substantial theoretical significance, as they explain why favorable technological, organizational, and environmental conditions may not automatically result in privacy compliance. Small and medium-sized enterprises (SMEs) need to first develop compliance readiness, and this readiness must then be translated into systematically structured business processes. Therefore, the conceptual model proposed in this study shifts the academic discourse from the perspective of compliance as a regulatory response to compliance as a capability-based managerial process.

This integrated approach also makes a significant contribution to the context of digital-based small and medium-sized enterprises (SMEs) in Indonesia. Digital-based SMEs are increasingly managing consumer personal data through online platforms, but most still operate with limited formal procedures. By investigating the TOE framework factors, compliance readiness constructs, Business Process Management capabilities, and privacy policy compliance in a single quantitative model, this study provides empirical evidence on how small and medium-sized enterprises can transition from reactive compliance to systematically structured privacy governance.

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Even though the TOE factors create the context upon which compliance with the privacy policies is established, they do not always lead to the practice of compliance. There could be digital SMEs that feel the force of regulation and have digital capabilities but still fail to adopt the policies due to their poor internal readiness and capability. With this in mind, it is imperative to understand how compliance readiness and BPM capability can mediate these drivers into practices.

Compliance readiness is expected to mediate the relationship between TOE factors and privacy policy compliance. Favorable technological, organizational, and environmental conditions may increase SME readiness, which in turn improves the likelihood of privacy policy compliance. This argument is consistent with readiness literature that views readiness as a connecting mechanism between implementation antecedents and outcomes (Rafferty et al., 2013; Shea et al., 2014). Therefore, the following hypothesis is proposed:

H6: Compliance readiness mediates the relationship between TOE factors and privacy policy compliance.

BPM capability is also expected to mediate the relationship between TOE factors and privacy policy compliance. TOE factors may encourage SMEs to formalize and control data related business processes, while BPM capability enables these processes to support compliance implementation. In this sense, BPM capability explains how contextual conditions are translated into operational compliance routines. Therefore, the following hypothesis is proposed:

H7: BPM capability mediates the relationship between TOE factors and privacy policy compliance.

In this research, we propose a sequential mediation model. It is believed that the Technology-Organization-Environment (TOE) factors will help increase the compliance readiness of an organization, which will further improve its BPM capacity, thus leading to compliance with privacy policies. This sequence of events is based on the rationale that SMEs need context first, then readiness, and then process capability to achieve sustainable privacy compliance. Thus, the hypothesis to be tested is:

H8: The constructs of compliance readiness and BPM capability mediate the effect of TOE factors on the compliance of privacy policies in sequence.

Figure 1 illustrates the proposed framework for the study. The research model conceptualizes compliance of privacy policies within digital SMEs as a dependent variable that arises due to various context-based variables, preparedness and capabilities of SMEs. TOE factors include technology, organization and environment aspects. Compliance readiness is the level of readiness of SMEs in terms of handling privacy policies, while BPM capability is the ability of SMEs to develop and improve data-related processes.

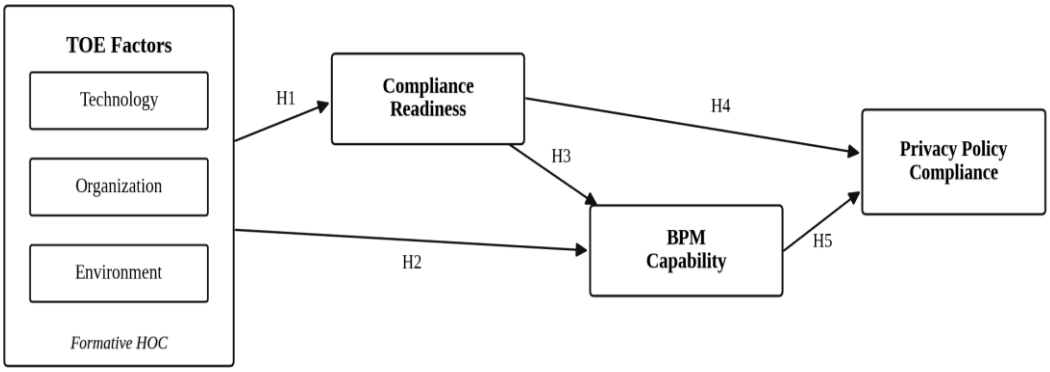


Fig 1. Research Framework

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Figure 1 shows the suggested research model. The direct causal linkages are represented as H1 to H5, while the indirect linkages which are mediated by compliance readiness and BPM capability are shown by H6 to H8. Hypotheses related to mediation effect are not indicated separately in the figure by using additional arrows, but rather they appear in the indirect relationships between the TOE variables and privacy policy compliance through the mediator variables.

Table 1. Thematic Mapping of Literature

Theme	Core argument	Key sources	Construct implication
Privacy policy compliance	Privacy is an organizational governance issue that affects trust, customer vulnerability, and firm outcomes.	Smith et al. (2011); Belanger & Crossler (2011); Martin et al. (2017); Milne & Culnan (2004)	Supports privacy policy compliance as the dependent variable.
Data protection capability	Regulatory compliance requires data management capabilities, infrastructure, routines, and organizational controls.	Tikkinen Piri et al. (2018); Labadie & Legner (2023)	Supports compliance as capability, not only legal obligation.
SME cybersecurity and awareness	SMEs require tailored awareness and capability building due to resource and knowledge limitations.	Bada & Nurse (2019)	Supports the SME specific context and need for readiness.
TOE factors	Technology, organization, and environment shape firm level adoption and strategic action.	Zhu et al. (2003); Low et al. (2011); Ramdani et al. (2009); Gangwar et al. (2015); Awa et al. (2015)	Supports TOE as exogenous contextual antecedent.
Compliance readiness	Readiness reflects commitment, efficacy, resources, and preparedness for implementation.	Weiner (2009); Holt et al. (2007); Rafferty et al. (2013); Shea et al. (2014); Lokuge et al. (2019)	Supports compliance readiness as internal mediator.
Compliance behavior	Compliance depends on awareness, beliefs, motivation, and routine.	Bulgurcu et al. (2010); Herath & Rao (2009); Ifinedo (2012); Vance et al. (2012)	Supports the behavioral foundation of compliance readiness.
BPM capability	BPM enables documentation, standardization, monitoring, and continuous process improvement.	Trkman (2010); Roglinger et al. (2012); vom Brocke et al. (2016); Schmiedel et al. (2014, 2020)	Supports BPM capability as operational mediator.

In combination, the previous studies have been informative on the dimensions of privacy compliance, technology adoption, organizational readiness, and business process capability. However, these different areas of investigation have grown separately, without coming together to create an integrated understanding of these areas. The TOE studies generally consider the contextual factors, while the readiness and BPM studies focus on the internal factors of process capability. Little has been done to bring together the three approaches to understand how the digital SMEs use technological, organizational, and environmental factors to achieve compliance with the privacy policies.

3. Research Method

This research uses the quantitative methodology and survey research design in order to investigate the interaction among various elements in the TOE framework, compliance readiness, BPM capabilities, and privacy policy compliance in digital SMEs. Instead of conducting the detailed examination of one particular instance, the study empirically evaluates the proposed theoretical framework based on the data gathered from the sample of SMEs using digital technologies in their operations.

Cross-sectional survey design was chosen since data collection was conducted once. It is suitable for analyzing the perceptions, preparedness, capacity, and practices of organizations. In this particular case, the company will be the unit of analysis while respondents will show the state of affairs in the company from their perceptions concerning business processes, digital activities, and data management practices.

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

The model that was developed was assessed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The reason why this analysis tool was chosen is that it considers several latent variables, mediation effects, as well as higher order constructs which include the factors of TOE. Moreover, PLS-SEM is usually seen as an appropriate tool for revealing and predicting connections between constructs.

Population of the study consisted of digital small and medium sized enterprises in Indonesia. For the purposes of this research, digital SMEs refer to small and medium sized enterprises which make use of digital technologies in their operations including e-commerce sites, social media sites, digital payment services, cloud applications, online order placement systems and customer management systems. The SMEs selected for this study are digital because they perform daily operational tasks involving the collection and processing of customers' information including names, contact details and addresses.

The respondents for this study comprised owners/managers/staff members from SMEs who had good knowledge about digital functions and data handling in the firm. The reason why this criterion is important is that not all employees are aware of how the customer's data is being collected, stored, used, and protected. In other words, the survey targeted those individuals who had knowledge about business and data privacy in the firm.

Purposive sampling method was applied in the present study. The criterion for selecting samples was based on the lack of public information showing that digital small and medium-sized enterprises (SMEs) in Indonesia use personal data processing. Samples were selected based on the following criteria: (1) the SME is categorized as a SME; (2) the SME uses some type of digital technology in their business operation; (3) the SME collects/uses customer data; and (4) the samples have significant knowledge about digital business and enterprise data handling.

The minimum sample size was calculated considering the demands related to PLS-SEM method and the complexity of the research model itself. As the model includes several structural relationships and there might be a mediation effect as well, it is important to have enough respondents to get reliable estimates. Thus, after rejecting the incomplete and irrelevant answers, the total number of valid answers amounted to 200.

Data collection has been conducted using an online questionnaire sent out to digital SMEs through business networks, alumni networks, professional contacts, and various online communications channels. Respondents have answered some screening questions to ensure that their businesses meet the inclusion criteria of the study before moving on to the main questions.

To address the concerns of the respondents, the questionnaire did not ask for any sensitive information, such as any business records or customer identities. The questions focused on organizational practices, readiness, process capabilities, and privacy policy compliance.

The questionnaire has been created based on the measurement constructs used in the past studies and adjusted to be applicable for measuring privacy policy compliance in digital SMEs. In order to make sure that all respondents can understand the questionnaire, all measurement items have been formulated using simple language without any technical or legal terms. It is due to the fact that despite the use of personal data in their operations, most SMEs might not know about privacy or compliance terminology. All measurement items were formulated using five-point Likert scale, where 1 = strongly disagree and 5 = strongly agree to ensure better completion of the questionnaire by SME respondents.

This study will focus on four primary constructs, which include TOE factors, compliance readiness, BPM capabilities, and privacy policy compliance. The TOE factors will be considered formative high-level constructs consisting of three dimensions, which are technology, organization, and environment. Technology is a dimension that shows how much digital systems enable data protection and monitoring. Organization is a dimension that demonstrates management commitment and resources for privacy activities, as well as

https://doi.org/10.35877/soshum5132

OPEN ACCESS

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

accountability. Environment is a dimension that shows external pressures, customer and partner expectations, and reputation issues.

Compliance readiness is a reflective construct that demonstrates awareness and readiness of SMEs to meet privacy-related requirements. Similarly, BPM capability is a reflective construct that represents the ability of organizations to document, standardize, monitor and improve business processes related to data handling. Privacy policy compliance is a reflective construct that shows how well SMEs comply with privacy-related policies and procedures.

Table 2. Measurement Items

Code	Items	Sources
TEC1	Our firm has adequate digital systems to manage and protect personal data.	Adapted from Zhu et al. (2003), Low et al. (2011), and Gangwar et al. (2015)
TEC2	The digital technology used by our firm supports access control to customer data.	
TEC3	Our information systems allow the firm to monitor data related activities.	
TEC4	Our firm regularly updates the digital systems used to protect personal data.	
TEC5	Our firm has backup and recovery mechanisms for personal data.	
ORG1	Management supports the implementation of privacy related policies.	Adapted from Low et al. (2011), Gangwar et al. (2015), and Hu et al. (2012)
ORG2	Our firm provides sufficient resources to support privacy compliance.	
ORG3	Our firm has clear responsibility for managing personal data.	
ORG4	Employees receive guidance or training on the proper handling of personal data.	
ORG5	Our firm periodically evaluates its personal data protection practices.	
ENV1	Data protection regulations encourage our firm to comply with privacy policies.	Adapted from Zhu et al. (2003), Low et al. (2011), Gangwar et al. (2015), and Herath and Rao (2009)
ENV2	Expectations from customers or business partners influence our firm's privacy practices.	
ENV3	Reputational risk motivates our firm to protect personal data properly.	
ENV4	Practices adopted by competitors or other firms encourage our firm to improve personal data protection.	
CR1	Our firm understands privacy related obligations.	Adapted from Holt et al. (2007), Bulgurcu et al. (2010), and Shea et al. (2014)
CR2	Our firm is ready to implement privacy policies in daily operations.	
CR3	Employees are aware of the importance of protecting personal data.	
CR4	Our firm is committed to complying with privacy related requirements.	
CR5	Our firm has the resources and capability needed to implement privacy related requirements.	
BPM1	Business processes related to data management are well documented.	Adapted from McCormack et al. (2009), Škrinjar and Trkman (2013), and Van Looy (2020)
BPM2	Our firm has clear procedures for handling customer data.	
BPM3	Data related business processes are monitored regularly.	
BPM4	Our firm evaluates and improves data related processes when needed.	
BPM5	Privacy requirements are integrated into our firm's routine business processes.	
PPC1	Our firm collects only personal data that are necessary for business activities.	Adapted from Herath and Rao (2009), Bulgurcu et al. (2010), and Ifinedo (2012, 2014)
PPC2	Our firm uses personal data only for the purposes for which they were collected.	
PPC3	Our firm does not share personal data with other parties without permission.	
PPC4	Access to personal data is limited to authorized personnel.	
PPC5	Our firm takes corrective action when errors or personal data breaches occur.	
PPC6	Our firm deletes or stops using personal data that are no longer needed.	

A total of 174 valid responses were included in the analysis. The sample size was considered adequate for PLS-SEM because an a priori statistical power analysis indicated that the minimum required sample size was substantially lower than the final sample obtained. Therefore, the statistical power was sufficient to detect the hypothesized relationships among

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

the constructs (Hair et al., 2021). Furthermore, PLS-SEM is particularly suitable for predictive research involving relatively moderate sample sizes and complex models with mediation effects.

The screening process aimed to check for data completeness, respondent eligibility, non-duplicates, and logic. As all items in the questionnaires were designed to be mandatory in the online survey tool, there were no missing values in the collected dataset. The duplicate answers were determined by comparing timestamp and respondents' information; thus, there were no duplicates in the dataset. Furthermore, each answer was analyzed on the basis of pre-established screening criteria in order to assure that the respondents were digital small and medium-sized enterprises using digital technology in their operations and having enough knowledge about their organizations' data management processes.

This study follows the two-step procedure outlined by Hair et al. (2022). First, the measurement model was checked using such measures as indicators' reliability, internal consistency reliability, convergent validity, and discriminant validity. The measures of internal consistency used in this study include Cronbach's alpha, rho_A, and composite reliability; convergent validity is measured through outer loadings and average variance extracted (AVE); discriminant validity is measured using the heterotrait–monotrait (HTMT) ratio. As for the formative higher-order construct (TOE Factor), collinearity is measured with the help of variance inflation factor (VIF), then outer weights and their significance were examined.

Second, the structural model was tested. In addition to collinearity, the diagnostics included path coefficients, coefficient of determination (R^2), effect size (f^2), predictive relevance (Q^2), and SRMR – the measure of model fit. The significance of the proposed relationships (including indirect and direct effects) was checked with the help of bootstrapping procedure, which involved 5,000 samples and bias-corrected confidence intervals.

4. Results and Discussion

There were 175 answers obtained through the online survey. After data screening, one answer was removed from further analysis because it failed to satisfy the set criteria for inclusion. This left 174 answers for analysis.

Table 3. Respondent Characteristics (n = 174)

Variable	Category	Frequency	Percentage (%)
Position in the business	Owner	151	86.8
	Manager	4	2.3
	Staff	8	4.6
	Other roles	11	6.3
Business age	<2 years	53	30.5
	2–5 years	64	36.8
	>5 years	57	32.8
Number of employees	1–4	163	93.7
	5–19	9	5.2
	≥20	2	1.1
Digital platforms used*	Social media	161	92.5
	Marketplace	75	43.1
	Delivery/aggregator platform	37	21.3
	Own website	30	17.2
	POS application	13	7.5
	No platform stated	1	0.6

The demographic and business details of the participants are summarized in Table 3 below. They were mostly business owners/managers actively involved in conducting digital business and managing personal data. The SMEs that participated in the study included various industries, and different digital tools such as social media sites, ecommerce sites, digital payments, and cloud applications were used by them.

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Table 4. Reflective Measurement Model Evaluation

Construct	Indicator	Loading	Cronbach's alpha	rho_A	Composite reliability	AVE
Technology	TEC1	0.923	0.944	0.947	0.957	0.816
	TEC2	0.883				
	TEC3	0.889				
	TEC4	0.922				
	TEC5	0.899				
Organization	ORG1	0.881	0.956	0.957	0.966	0.850
	ORG2	0.931				
	ORG3	0.957				
	ORG4	0.940				
	ORG5	0.899				
Environment	ENV1	0.933	0.941	0.941	0.958	0.851
	ENV2	0.897				
	ENV3	0.935				
	ENV4	0.924				
Compliance Readiness	CR1	0.908	0.963	0.964	0.971	0.871
	CR2	0.907				
	CR3	0.936				
	CR4	0.961				
	CR5	0.952				
BPM Capability	BPM1	0.941	0.972	0.973	0.978	0.900
	BPM2	0.955				
	BPM3	0.966				
	BPM4	0.956				
	BPM5	0.925				
Privacy Policy Compliance	PPC1	0.862	0.955	0.955	0.964	0.817
	PPC2	0.936				
	PPC3	0.915				
	PPC4	0.930				
	PPC5	0.938				
	PPC6	0.837				

Source: SmartPLS output processed by the authors.

This measurement model shows that reliability and convergent validity of all the reflective constructs are satisfactory. The outer loadings exceed the proposed threshold of 0.708 as the values are in the range of 0.837 and 0.966. This means that there is a high relationship between the indicator and construct. Cronbach's alpha values are within the range of 0.941 to 0.972, whereas the composite reliability values are in the range of 0.957 to 0.978. Both of these values are higher than the recommended value of 0.70. Average Variance Extracted (AVE) values are higher than the minimum value of 0.50 which is 0.816 to 0.900.

Discriminant validity was evaluated using the heterotrait-monotrait ratio. As shown in Table 5, the HTMT estimates among the reflective constructs ranged from 0.626 to 0.844. All values were below the conservative threshold of 0.850, indicating that the constructs were empirically distinguishable from one another (Henseler et al., 2015). The highest HTMT value was observed between Compliance Readiness and BPM Capability (0.844), which is theoretically reasonable because organizational readiness is expected to support the development of process capability. Nevertheless, the value remained below the threshold, confirming adequate discriminant validity.

Table 5. Discriminant Validity: Heterotrait-Monotrait Ratio

Construct	(1)	(2)	(3)	(4)	(5)	(6)
(1) Technology	—					
(2) Organization	0.789	—				
(3) Environment	0.749	0.843	—			
(4) Compliance Readiness	0.683	0.801	0.811	—		
(5) BPM Capability	0.683	0.800	0.792	0.844	—	
(6) Privacy Policy Compliance	0.626	0.719	0.804	0.737	0.732	—

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Discriminant validity was evaluated using the heterotrait-monotrait ratio. As shown in Table 5, the HTMT estimates among the reflective constructs ranged from 0.626 to 0.844. All values were below the conservative threshold of 0.850, indicating that the constructs were empirically distinguishable from one another (Henseler et al., 2015). The highest HTMT value was observed between Compliance Readiness and BPM Capability (0.844), which is theoretically reasonable because organizational readiness is expected to support the development of process capability. Nevertheless, the value remained below the threshold, confirming adequate discriminant validity.

The formative higher-order construct was assessed separately by examining the significance and collinearity of its three dimensions. Table 6 shows that Technology, Organization, and Environment had positive and statistically significant weights in forming TOE Factors. Organization provided the largest contribution (β=0.415)), followed by Technology (β=0.354)) and Environment (β=0.323)). Their VIF values ranged from 2.492 to 3.422, remaining below the threshold of 5.000. Therefore, no critical collinearity problem was identified, and all three dimensions were retained as formative components of TOE Factors.

Table 6. Formative Higher-Order Construct Assessment

Dimension	Weight	t-statistic	p-value	VIF	Decision
Technology → TOE Factors	0.354	31.138	<0.001	2.492	Retained
Organization → TOE Factors	0.415	28.232	<0.001	3.422	Retained
Environment → TOE Factors	0.323	26.115	<0.001	2.995	Retained

Source: SmartPLS output processed by the authors.

Overall, the results establish satisfactory indicator reliability, internal consistency reliability, convergent validity, discriminant validity, and formative measurement quality. The measurement model was therefore considered adequate for evaluating the structural relationships and testing the proposed hypotheses.

Following the assessment of the measurement model, the structural model was evaluated using the coefficient of determination ((R^2)), effect size ((f^2)), predictive relevance ((Q^2)), and the standardized root mean square residual (SRMR). The results are summarized in Tables 7 and 8.

The model explained 64.1% of the variance in Compliance Readiness ((R^2=0.641)), 72.6% of the variance in BPM Capability ((R^2=0.726)), and 54.9% of the variance in Privacy Policy Compliance ((R^2=0.549)). The corresponding adjusted (R^2) values were 0.639, 0.722, and 0.544, respectively. These results indicate moderate to substantial explanatory power. In particular, the relatively high variance explained in BPM Capability suggests that contextual TOE conditions and internal compliance readiness jointly provide a strong explanation of SMEs' ability to manage data-related business processes.

Table 7. Explanatory and Predictive Power of the Structural Model

Endogenous construct	(R^2)	Adjusted (R^2)	(Q^2)
Compliance Readiness	0.641	0.639	0.554
BPM Capability	0.726	0.722	0.648
Privacy Policy Compliance	0.549	0.544	0.438

Source: SmartPLS output processed by the authors.

Predictive relevance was examined through the blindfolding procedure. The (Q^2) values were 0.554 for Compliance Readiness, 0.648 for BPM Capability, and 0.438 for Privacy Policy Compliance. All values were well above zero, showing that the model had meaningful predictive relevance for each endogenous construct. The (R^2) and (Q^2) values generated for TOE Factors were not interpreted because they resulted from its specification as a formative higher-order construct rather than from its role as a substantive endogenous outcome.

Furthermore, the significance of each independent variable was evaluated using the f^2 effect size. It was found that the effect size of TOE Factors on Compliance Readiness was large (f^2 = 1.786), which suggests that technology, organization, and environment factors play an

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

important role in the formation of compliance readiness. The effect of TOE Factors on BPM Capability was medium (f^2 = 0.211). In turn, the effect of Compliance Readiness on BPM Capability was medium (f^2 = 0.321), whereas the effect of Compliance Readiness on Privacy Policy Compliance was small (f^2 = 0.114). BPM Capability had a small effect on Privacy Policy Compliance (f^2 = 0.109).

Table 8. Effect Size Assessment

Structural relationship	(f^2)	Interpretation
TOE Factors → Compliance Readiness	1.786	Large
TOE Factors → BPM Capability	0.211	Medium
Compliance Readiness → BPM Capability	0.321	Medium
Compliance Readiness → Privacy Policy Compliance	0.114	Small
BPM Capability → Privacy Policy Compliance	0.109	Small

Note: (f^2) values of 0.02, 0.15, and 0.35 represent small, medium, and large effects, respectively. Source: SmartPLS output processed by the authors.

The model fit was tested using the Standardized Root Mean Square Residual (SRMR). In this case, the saturated model showed an SRMR value of 0.071, which falls below the stringent cutoff point of 0.080. On the other hand, the estimated model returned an SRMR value of 0.083. Even though this value surpasses the more stringent 0.080 standard, it still falls below the less stringent one of 0.100. Taking into account the results of explanation and prediction, the model shows adequate fit.

Hypotheses were tested using bootstrap methodology with 5,000 resamples. For statistical significance of association, t-statistic needed to be greater than 1.96, p-value less than 0.05, and 95% confidence intervals not including zero. Table 9 shows that all five hypotheses were supported by evidence.

Table 9. Direct Hypothesis Testing Results

Hypothesis	Structural relationship	β	t-value	p-value	95% confidence interval	Decision
H1	TOE Factors → Compliance Readiness	0.801	21.826	<0.001	[0.723, 0.861]	Supported
H2	TOE Factors → BPM Capability	0.402	4.167	<0.001	[0.218, 0.576]	Supported
H3	Compliance Readiness → BPM Capability	0.495	4.909	<0.001	[0.288, 0.684]	Supported
H4	Compliance Readiness → Privacy Policy Compliance	0.393	3.174	0.002	[0.153, 0.640]	Supported
H5	BPM Capability → Privacy Policy Compliance	0.385	2.934	0.003	[0.120, 0.613]	Supported

Source: SmartPLS bootstrapping output processed by the authors.

Factors of TOE had an impressive impact on the dependent variable, Compliance Readiness (β = 0.801, t = 21.826, p < 0.001), thus proving hypothesis one. It was the most significant path in the proposed model which shows that technological, organizational, and environmental factors play a crucial role in addressing privacy needs for digital SMEs.

TOE Factors also positively affected BPM Capability (β = 0.402), (t = 4.167), (p < 0.001)); therefore, H2 was supported. Compliance Readiness had a significant positive effect on BPM Capability (β = 0.495), (t = 4.909), (p < 0.001)), supporting H3. This result indicates that stronger internal readiness is associated with a greater ability to document, monitor, and improve data-related business processes.

The effects of Compliance Readiness (β = 0.393), (t=3.174), (p=0.002)) and BPM Capability (β=0.385), (t=2.934), (p=0.003)) on Privacy Policy Compliance were also positive and significant. Accordingly, H4 and H5 were supported. The confidence intervals for all structural paths remained above zero, confirming the stability of the estimated relationships.

The mediating effects were assessed using the specific indirect effects generated through bootstrapping with 5,000 resamples. An indirect relationship was considered significant when its p-value was below 0.05 and the 95% confidence interval did not include zero. Table 10 shows that all three proposed mediation hypotheses were supported.

https://doi.org/10.35877/soshum5132

OPEN ACCESS

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Table 10. Mediation Testing Results

Hypothesis	Indirect relationship	β	t-value	p-value	95% confidence interval	Decision
H6	TOE Factors → Compliance Readiness → Privacy Policy Compliance	0.314	3.112	0.002	[0.116, 0.522]	Supported
H7	TOE Factors → BPM Capability → Privacy Policy Compliance	0.155	2.325	0.020	[0.043, 0.293]	Supported
H8	TOE Factors → Compliance Readiness → BPM Capability → Privacy Policy Compliance	0.153	2.348	0.019	[0.055, 0.308]	Supported

Source: SmartPLS bootstrapping output processed by the authors.

Compliance Readiness significantly mediated the relationship between TOE Factors and Privacy Policy Compliance (β=0.314), (t=3.112), (p=0.002)), supporting H6. This result suggests that favorable technological, organizational, and environmental conditions are more likely to improve privacy compliance when they first strengthen the firm's awareness, commitment, and preparedness to implement privacy requirements.

The indirect effect through BPM Capability was also significant (β = 0.155, t = 2.325, p = 0.020), thus, H7 was confirmed. It seems that TOE conditions have an impact on privacy compliance in terms of assisting the SMEs in developing a more structured process related to the documentation, monitoring, and improvement of data-related activities.

The sequential indirect effect through Compliance Readiness and BPM Capability was also significant and positive (β = 0.153, t = 2.348, p = 0.019), therefore, H8 was supported. Thus, it can be seen that the presence of context alone is not enough to ensure consistent privacy practices. Instead, context initially contributes to the readiness of the organization, which further helps to improve process capability and ensures compliance implementation.

Since the structural model does not include the direct link between TOE Factors and Privacy Policy Compliance, the mediational effect was based on the significance of specific indirect effects instead of the classification of the latter as partial or full mediation. Overall, it can be said that Compliance Readiness and BPM Capability work as essential mediating variables in the link between TOE conditions and Privacy Policy Compliance.

It is seen from the results that the compliance of privacy policies in digital SMEs is influenced by a series of steps such as contextual support, organizational readiness, and process capability. All hypotheses have been validated, and the model explains 54.9% of the variation in Privacy Policy Compliance. This finding highlights the fact that privacy compliance goes beyond being a mere reaction to regulations since it occurs where SMEs have supportive technology, organization, and environment context, along with readiness, which is translated into process capability.

Among the TOE factors, those of Organization had the greatest impact on Compliance Readiness (β = 0.801). In other words, it can be concluded that the readiness depends strongly on the external context of the firm. Technical context includes digital systems that provide an opportunity to control and monitor personal data, while organizational context means having resources and accountability. Environmental context, in its turn, raises the significance of privacy protection. Formative assessment also showed that the contribution of Organization was the highest, followed by Technology and Environment. Thus, it may be inferred that digital tools and regulatory pressure would not work without managerial commitment and internal resources.

The results build on previous TOE literature, where technological, organizational, and environmental factors have been extensively applied to explain decision making concerning technology adoption and implementation (Gangwar et al., 2015b; Low et al., 2011; Zhu et al., 2003). In this case, TOE factors do not only encourage the adoption of the technology; rather, they lay the foundation for SMEs becoming aware of privacy requirements,

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

committing to compliance, and developing assurance of their capability to act. This finding is in agreement with the organizational readiness theory by Weiner (2009), where he states that successful organizational change requires both commitment and capability to implement.

The factors of TOE had a positive impact on BPM capabilities (β = 0.402). The point is that digital infrastructure helps in documenting and monitoring the processes related to data, and management support allows companies to invest resources and distribute tasks. Pressure from regulators, customers, and business partners can also push companies to develop standardized procedures. Therefore, the contribution of TOE goes beyond the explanation of adoption. In the case of digital SMEs, favorable circumstances are also helpful for developing the necessary capability.

The impact of Compliance Readiness had a stronger effect on BPM Capability (β = 0.495) compared to the impact of TOE Factors directly on BPM Capability. Such a difference carries importance on the theoretical level. When conditions provide tools, pressure, and organizational support, there is a higher probability that formalization will happen only when the organization is ready for the change. Knowledge about the need for privacy, the willingness of managers, awareness of employees, and availability of resources create the internal drive that will enable the documentation, allocation of roles, monitoring, and fixing of process weaknesses.

This supports the argument that readiness is not limited to a psychological mindset alone. Readiness can bring about practical changes in organizations in small businesses. This finding is consistent with the literature on readiness, which finds that commitment, efficacy, managerial support, and availability of resources contribute to implementation success (Holt et al., 2007; Shea et al., 2014; Weiner, 2009). This finding also implies that privacy training in small businesses must go beyond awareness. Readiness efforts must help SMEs determine roles and assess resources as well as develop implementation strategies from overall intentions.

There were two constructs which had considerable impact on Privacy Policy Compliance. First, Compliance Readiness positively impacted compliance (β = 0.393), which is expected since greater awareness, commitment and capability translate into better compliance with privacy policies by SMEs in day-to-day operations. Second, Compliance Readiness fits well with the existing theory of information security compliance which suggests that awareness, beliefs, motivation and perceived effectiveness play important roles in fostering compliant behavior (Bulgurcu et al., 2010; Herath & Rao, 2009; Ifinedo, 2012).

The impact of BPM capability is even greater on Privacy Policy Compliance (β = 0.385). Even though the magnitude of the effect is a bit lower compared to Compliance Readiness, it supports the hypothesis that compliance needs to become a part of the organization's routine. Digital SMEs have to collect personal data when receiving orders, paying for them, communicating with clients, storing transaction history and managing client complaints. Once those processes are described, automated, monitored and optimized, all privacy regulations will become integral elements of the organization's activities instead of something done as a reaction to external pressures. This finding is consistent with the BPM research that considers process capability as a basis of organizational consistency and performance (Roglinger et al., 2012; Schmiedel et al., 2014; Trkman, 2010). It is also supported by Labadie and Legner (2023) as they argue that only organizational data management capabilities can provide sustainability of data protection compliance.

These results provide further insight into how the TOE factors impact on privacy compliance through their mechanisms. The variable "Compliance Readiness" was found to mediate the TOE-Privacy Policy Compliance relationship (β = 0.314). This is the highest indirect effect, suggesting that the most direct way in which contextual factors impact on privacy compliance is by increasing readiness for action on the part of the organization. While the organization may have the right tools and feel pressured to take action due to regulation or customers,

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

these factors do not hold much importance without the managers and employees knowing what needs to be done.

TOE factors' influence on privacy compliance policies is mediated by BPM capability (β = 0.155). This means that through contextual support, one can improve the level of compliance of companies since such support helps to achieve formality and control of the processes involved. More importantly, however, the mediation is sequential because of the influence of compliance readiness and BPM capability (β = 0.153). In other words, from the mediation above, it is clear that contextual support leads to readiness, readiness improves process capability, and process capability ensures compliance.

The results from the mediation analysis represent the theoretical contribution of the paper. Previous studies of the TOE framework have mainly looked into how contextual factors influence adoption or implementation effects. The present study shows how things happen in between the said conditions and compliance result. Through the integration of TOE factors, Compliance readiness, and BPM capability, the new model changes the conversation from compliance being a response to the need to comply to compliance being a managerial process through capability. In addition, the paper shows how the theory of organizational readiness can be tied to BPM by showing that readiness becomes more useful once it is translated to business processes.

As a manager, the owners of SMEs need to ensure that privacy compliance is not perceived as just another single task, either legally or technically. Simply having secure software will not be enough without adequate employee training, without defined roles, and without well-defined methods of handling data. A more practical approach to privacy compliance requires commitment and technology support, followed by organizational preparedness and, finally, documenting the process involved in processing personal information.

These results have implications for policymakers as well as organizations that help small and medium-sized enterprises (SMEs). Training programs that communicate the regulatory requirements alone may increase knowledge but will not bring about lasting compliance. The training should involve process guides, identifying the individuals responsible for managing data, conducting risk assessments, and helping to document and improve everyday tasks. It seems like such training is more relevant for SMEs with limited budgets than compliance programs for large businesses.

All in all, from the results presented, it becomes clear that the implementation of privacy policies has a higher potential for sustainability in cases where both external and internal contexts are integrated through organizational readiness and process capability. The TOE context defines the basis, Compliance Readiness equips the firm with the capability to move into action, while BPM Capability turns such capability into action.

5. Conclusion

This research explored the influence of TOE Factors on the compliance of Indonesian digital SMEs' privacy policies through compliance readiness and BPM capabilities. The findings revealed that the TOE Factors positively enhance Compliance Readiness and directly influence BPM Capability. Compliance Readiness influences BPM Capability and Privacy Policy Compliance positively, while BPM Capability positively influences Privacy Policy Compliance. These influences combined account for 54.9% of the variance in privacy policy compliance.

The findings from the mediation test offer the ultimate findings of the study. Good TOE conditions do not necessarily ensure compliance with privacy rules. It is the process within the organization that influences this effect. Compliance Readiness allows small medium enterprises to be aware of the need for privacy, invest in resources, and prepare their employees, while BPM Capability transforms this readiness into a process of data handling. The mediation effect shows that privacy compliance is a progressive process from context to preparedness to capability.

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

The results enhance the TOE framework by indicating that context is relevant when related to readiness and process capability. The results further expand organizational readiness theory by suggesting that readiness influences compliance both directly and indirectly, where readiness leads to the creation of more robust processes which then enable compliance. From a management standpoint, it is important for digital SMEs not to think of privacy compliance as merely an obligation or just a technical challenge. Privacy compliance needs management commitment, accountability, awareness, and regular processes involving personal data management.

Compliance programs for policymakers and institutions supporting SMEs must go beyond regulatory socialization. Help in practical terms is required through easy-to-follow privacy processes, assignment of roles, documentation of process, monitoring systems, and corrective action plans that fit the capacity of SMEs. There are limitations in the research such as the cross-sectional study design, purposive sampling technique, and the use of self-reports from 174 respondents. Further research may use longitudinal design, wider sample, objective measures of compliance, and comparison across SMEs to see how the relationships persist.

References

Awa, H. O., Ojiabo, O. U., & Emecheta, B. C. (2015). Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs. Journal of Enterprise Information Management, 28(4), 520–543. https://doi.org/10.1108/JEIM-04-2013-0012

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly, 35(4), 1017–1041. https://doi.org/10.2307/41409971

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548. https://doi.org/10.2307/25750690

Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2018). Introduction to Business Process Management. In M. Dumas, M. La Rosa, J. Mendling, & H. A. Reijers, Fundamentals of Business Process Management (pp. 1–33). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-56509-4_1

Gangwar, H., Date, H., & Ramaswamy, R. (2015a). Understanding determinants of cloud computing adoption using an integrated TAM TOE model. Journal of Enterprise Information Management, 28(1), 107–130. https://doi.org/10.1108/JEIM-08-2013-0065

Gangwar, H., Date, H., & Ramaswamy, R. (2015b). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. Journal of Enterprise Information Management, 28(1), 107–130. https://doi.org/10.1108/JEIM-08-2013-0065

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook. Springer International Publishing. https://doi.org/10.1007/978-3-030-80519-7

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Holt, D. T., Armenakis, A. A., Feild, H. S., & Harris, S. G. (2007). Readiness for organizational change: The systematic development of a scale. The Journal of Applied Behavioral Science, 43(2), 232–255. https://doi.org/10.1177/0021886306295295

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU GDPR. Journal of Information Technology, 38(1), 16–44. https://doi.org/10.1177/02683962221141456

Lokuge, S., Sedera, D., Grover, V., & Xu, D. (2019). Organizational readiness for digital innovation: Development and empirical calibration of a construct. Information & Management, 56(3), 445–461. https://doi.org/10.1016/j.im.2018.09.001

Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. Industrial Management & Data Systems, 111(7), 1006–1023. https://doi.org/10.1108/02635571111161262

Martin, K. D., Borah, A., & Palmatier, R. W. (2017a). Data Privacy: Effects on Customer and Firm Performance. Journal of Marketing, 81(1), 36–58. https://doi.org/10.1509/jm.15.0497

Martin, K. D., Borah, A., & Palmatier, R. W. (2017b). Data privacy: Effects on customer and firm performance. Journal of Marketing, 81(1), 36–58. https://doi.org/10.1509/jm.15.0497

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read or do not read online privacy notices. Journal of Interactive Marketing, 18(3), 15–29. https://doi.org/10.1002/dir.20009

Oliveira, T., & Martins, M. F. (2011). Literature Review of Information Technology Adoption Models at Firm Level. 14(1).

Rafferty, A. E., Jimmieson, N. L., & Armenakis, A. A. (2013). Change readiness: A multilevel review. Journal of Management, 39(1), 110–135. https://doi.org/10.1177/0149206312457417

Ramdani, B., Kawalek, P., & Lorenzo, O. (2009). Predicting SMEs' adoption of enterprise systems. Journal of Enterprise Information Management, 22(1/2), 10–24. https://doi.org/10.1108/17410390910922796

Roglinger, M., Poppelbuss, J., & Becker, J. (2012). Maturity models in business process management. Business Process Management Journal, 18(2), 328–346. https://doi.org/10.1108/14637151211225225

Schmiedel, T., Recker, J., & Vom Brocke, J. (2020). The relation between BPM culture, BPM methods, and process performance: Evidence from quantitative field studies. Information & Management, 57(2), 103175. https://doi.org/10.1016/j.im.2019.103175

Schmiedel, T., Recker, J., & vom Brocke, J. (2020). The relation between BPM culture, BPM methods, and process performance: Evidence from quantitative field studies. Information & Management, 57(2), 103175. https://doi.org/10.1016/j.im.2019.103175

Schmiedel, T., vom Brocke, J., & Recker, J. (2014). Development and validation of an instrument to measure organizational cultures' support of Business Process Management. Information & Management, 51(1), 43–56. https://doi.org/10.1016/j.im.2013.08.005

Shea, C. M., Jacobs, S. R., Esserman, D. A., Bruce, K., & Weiner, B. J. (2014). Organizational readiness for implementing change: A psychometric assessment of a new measure. Implementation Science, 9, 7. https://doi.org/10.1186/1748-5908-9-7

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. MIS Quarterly, 35(4), 989–1015. https://doi.org/10.2307/41409970

Tikkinen Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Trkman, P. (2010). The critical success factors of business process management. International Journal of Information Management, 30(2), 125–134. https://doi.org/10.1016/j.ijinfomgt.2009.07.003

https://doi.org/10.35877/soshum5132

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information & Management, 49(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

vom Brocke, J., Zelt, S., & Schmiedel, T. (2016). On the role of context in business process management. International Journal of Information Management, 36(3), 486–495. https://doi.org/10.1016/j.ijinfomgt.2015.10.002

Weiner, B. J. (2009). A theory of organizational readiness for change. Implementation Science, 4(1), 67. https://doi.org/10.1186/1748-5908-4-67

Zhu, K., Kraemer, K. L., & Xu, S. (2003). Electronic business adoption by European firms: A cross country assessment of the facilitators and inhibitors. European Journal of Information Systems, 12(4), 251–268. https://doi.org/10.1057/palgrave.ejis.3000475