IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 14, No. 5, October, 2024, pp. 1559-1567
Journal homepage: http://iieta.org/journals/ijsse

Assessing Indonesian MSMEs' Awareness of Personal Data Protection by PDP Law and ISO/IEC 27001:2013

Endah Fuji Astuti*, Achmad Nizar Hidayanto, Sabila Nurwardani, Ailsa Zayyan Salsabila

Computer and Science Faculty, University of Indonesia, Jakarta 10430, Indonesia

Corresponding Author Email: endah.fuji@ui.ac.id

https://doi.org/10.18280/ijsse.140523

Received: 20 August 2024
Revised: 10 October 2024
Accepted: 17 October 2024
Available online: 31 October 2024

Keywords:
personal data protection, descriptive statistical analysis, Indonesia MSMEs, awareness, PDP Law Indonesia, ISO/IEC 27001:2013

ABSTRACT

Digital technology, while streamlining business operations, also poses significant risks by recording vast amounts of data. This study evaluates the awareness and compliance of Indonesian MSMEs with the Personal Data Protection (PDP) Law and ISO/IEC 27001:2013 standards, highlighting areas needing improvement. Using a quantitative approach, an online questionnaire was distributed to 126 MSMEs across Indonesia to assess legal awareness, consent management, data processing, and governance structures. The analysis, employing descriptive statistics and a Likert scale, reveals a low awareness of the PDP Law (mean score: 3.13) and partial compliance in consent management (mean score: 3.49). While data processing shows strengths (mean score: 3.71), weaknesses in third-party agreements (mean score: 2.67) and the appointment of Data Protection Officers (mean score: 2.98) indicate governance gaps. The findings underscore the struggle of Indonesian MSMEs in implementing crucial data protection practices. The study recommends investing in legal and data protection training, formalizing data agreements, appointing Data Protection Officers, conducting regular audits, and improving data breach management. These steps are vital for fostering a data protection culture and ensuring business sustainability in the digital age.

1. INTRODUCTION

During the COVID-19 pandemic in Indonesia, a significant shift in business models occurred as customer behavior evolved. People increasingly turned to digital platforms for a variety of activities, including shopping and communication [1, 2]. This surge in digital engagement has greatly enhanced the ability of Micro, Small, and Medium Enterprises (MSMEs) to market their products globally. However, the widespread use of digital technology presents both opportunities and challenges. While it simplifies many business operations, it also creates vulnerabilities by digitally recording a vast amount of information about these activities [3].

As a result, concerns about data security have emerged, particularly with regard to the personal information customers share during e-commerce transactions. Customers now face the challenge of ensuring their data is securely handled by MSMEs [4, 5]. To mitigate risks, it is crucial that only authorized users have access to customer data, preventing unauthorized access and potential misuse [6].

Cybersecurity threats are a growing concern for Indonesian MSMEs. According to Cisco Secure, 33% of cyber incidents and 68% of cyber threats target these businesses, with some suffering losses of up to IDR 7.6 billion annually [7]. High-profile data breaches have affected major platforms like Tokopedia, where more than 91 million user accounts and 7 million merchant records were compromised. Similarly, 13 million Bukalapak accounts and 73 million user records from various platforms have been leaked on the dark web, exposing sensitive information such as user IDs, email addresses, and personal identification details [8]. These incidents highlight the ongoing vulnerability of Indonesia's digital ecosystem to cyber threats and the critical need for improved security measures.

This research was conducted in the context of securing online e-commerce transactions. During transactions, customers with a better understanding seek clear evidence about safe online shopping [9]. Information security compliance behavior is influenced by the state of knowledge and awareness [10]. To guarantee minimum standards of data protection collected by MSMEs, the Indonesian PDP Law 2022, Number 27, needs to be used alongside data protection procedures [11]. To address MSME compliance with the PDP Law, this research investigates the awareness of MSMEs in Indonesia regarding their compliance using the GDPR implementation approach for MSMEs applied in Europe [12-14]. By adopting constructs from previous research [14, 15], this research significantly contributes to providing personal data security managed by MSMEs. This study also explores the extent to which the current awareness of personal data protection among MSMEs aligns with international information security standards set out in ISO/IEC 27001:2013, providing information protection standards for customers and MSMEs [16].

Regarding personal data protection through GDPR implementation in the EU, research by Leite et al. [12] states that enterprises more educated about GDPR will overcome emerging obstacles. In other related research, a lack of awareness about data protection policies, SME requirements, and rights impeded companies from adjusting to new legislation, causing delays in compliance [14]. It was also strongly argued by Bharti and Aryal [13] that the EU allocated EUR 6.3 million to boost data protection awareness for SMEs. Due to limited technical knowledge against threats and vulnerabilities of cybercrime, ISO/IEC 27001:2013, as an Information Security Management System, plays an essential role in protecting SMEs by providing security guidelines and fulfilling legal responsibilities [17]. Through ISO/IEC 27001:2013, SMEs gain increased awareness of the importance of security aligned with business objectives [18]. The five papers reviewed have common points, and they all agree that awareness about GDPR is important for SMEs to comply with the law and avoid potential risks and penalties.

Previous research on personal data privacy in Indonesia [8, 19] shares similar perspectives and scopes on personal data privacy in Indonesia and the need for comprehensive regulation and protection. However, unlike the GDPR and ISO/IEC 27001:2013, there has been no discussion regarding research on MSMEs' awareness of personal data protection. After searching respectable international journal databases, the author discovered no research discussing MSME awareness of data privacy protection in Indonesia. Because of this research gap, the following research question (RQ) can be formulated: "How is the awareness of Personal Data Protection among Indonesian MSMEs?"

This research aims to determine the awareness of MSMEs to comply with PDP Law Indonesia and ISO/IEC27001:2013 standard, which is very important to reduce the risk of customer data leaks which will have an impact on business. The research uses quantitative methods of a Likert scale questionnaire will be utilized to determine the issue. This study Indonesian MSMEs employ information technology. The respondent is not only the owner of the MSMEs but also a worker, to gain a different perspective from the Data Controller of Personal in controlling the processing of personal data and the Data Processor of Personal in carrying out the processing of personal data on behalf of the Personal Data Controller. By knowing these aspects in depth, this study will not only assess awareness but also suggest practical actions that can help MSMEs avoid potential data leaks. These findings are expected to improve customer data protection practices stored and used by MSMEs for their business needs.

2. METHODOLOGY

2.1 Methodology questionnaire design

This research adopts a quantitative approach through the use of an online questionnaire to collect data from Micro, Small, and Medium Enterprises (MSMEs) in Indonesia that utilize cloud services and marketplace platforms for marketing their products. The primary goal of the survey is to assess MSMEs' awareness and understanding of personal data protection, specifically within the context of the General Data Protection Regulation (GDPR) framework, Indonesian Personal Data Protection Law (PDP Law), and ISO/IEC 27001:2013. The alignment of data protection frameworks is shown in Table 1, referencing previous research [8, 14, 15, 19-21].

Table 1. Data protection framework alignment (GDPR EU, PDP Indonesia, and ISO/IEC 27001:2013)

Topic [14, 15]	Description [14, 15]	Art. GDPR [14, 15]	Art. PDP [8, 19, 20]	ISO/IEC 27001:2013 Annex A – Security Controls [21]	
Knowledge of law	Knowledge of law	-	Art. 1, Art. 2	A.18.1.1	Identification of applicable legislation and contractual requirements
Consent from data owner	Obtaining the consent of collecting or processing their personal data	Art. 6,7,13	Art. 20-22	A.8.2.3	Handling of Personally Identifiable Information (PII)
Processing fundamental	Processing personal data in accordance with the principles of the law	Art. 5	Art. 5, Art. 28	A.8.1.1, A.9.4.1	Inventory of assets
Record of processing action	An official list or record regarding of processing activity	Art. 30	Art. 60n, Art. 39	A.12.4.1, A.12.4.3	Event logging, administrator and operator logs
Workforce law	Compliance with workplace environment law	Art. 88	Art. 39	A.7.1.2, A.7.2.2	Terms and conditions of employment, education, training, and awareness of information security
Authority of the data owner	Providing owner with access to their private data	Art. 15, 16, 17, 19, 20, 21, 22	Art. 24, Art. 21-22, 16e	A.8.2.3	Handling of Personally Identifiable Information (PII)
DPO (Data Protection Officer)	Appointing DPO to ensure organization compliance.	Art. 37, 38, 39	Art. 53 clause 1	A.6.1.1	Roles and responsibilities within the organization
Secureness of processing data	fulfil the security step of data processing	Art.32	Art. 35	A.13.1.1, A.13.2.3	Network controls, electronic messaging
Written Contracts	Entering into contracts with processors to ensure personal data protection	Art. 28	Art. 60n	A.15.1.2	Addressing security within supplier agreements
Pass on the personal data to other countries	Ensuring that transfers of personal data to third countries are made by the law	Art 44, 45, 46	Art. 56	A.15.1.1, A.15.1.3	Information security policy for supplier relationships, Information and communication technology supply chain
Obedience of data regulator	Being accountable for compliance with the law	Art.24	Art. 54 clause 1b, Art. 34	A.18.1.4	Privacy and protection of personally identifiable information
Disclosure to the officials about the breach of personal data	Notifying the officials about data breaches	Art.33	Art. 60l, Art. 46	A.16.1.1, A.16.1.2	Responsibilities and procedures, reporting information security events

The questionnaire was constructed using a framework based on EU GDPR awareness, harmonized with Indonesia's PDP Law, and aligned with ISO/IEC 27001:2013 (Annex A), which outlines security controls aimed at protecting the confidentiality, integrity, and availability of information. To ensure clarity and readability, the questionnaire underwent a readability assessment before being distributed. The instrument was also tested for validity and reliability using the same sample as the final survey respondents. The results of the validity and reliability tests, which meet established criteria, are shown in Tables 2 and 3. A Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree) was employed to quantify respondents' perceptions.

Table 2. Reliability measurement results

Item	Coefficient	Item	Coefficient
V1	0.949	V11	0.948
V2	0.950	V12	0.947
V3	0.952	V13	0.950
V4	0.949	V14	0.948
V5	0.948	V15	0.953
V6	0.948	V16	0.951
V7	0.948	V17	0.950
V8	0.947	V18	0.948
V9	0.947	V19	0.947
V10	0.947	V20	0.948

Item V1-V20 can be seen in Table 7

Table 3. Validity measurement results

Item	r Value	Item	r Value
V1	0.683	V11	0.748
V2	0.648	V12	0.823
V3	0.526	V13	0.648
V4	0.734	V14	0.778
V5	0.748	V15	0.446
V6	0.763	V16	0.588
V7	0.774	V17	0.633
V8	0.808	V18	0.722
V9	0.848	V19	0.804
V10	0.807	V20	0.793

Item V1 to V20 can be seen in Table 7

2.2 Sampling methodology and data collection

This study utilizes a non-probability sampling method, specifically voluntary sampling, where potential respondents self-select into the study based on their willingness and qualification to meet the survey's criteria. This approach helps improve data quality by ensuring that respondents are not only willing to participate but also relevant to the study's objectives. The target population includes MSMEs operating in Indonesia that use cloud services and marketplace platforms. Both MSME owners and workers were included in the respondent pool to provide different perspectives on personal data protection. Owners represent the role of the Data Controller (responsible for controlling the data processing), while workers may serve as Data Processors (processing data on behalf of the Data Controller). The questionnaire was distributed online through Google Forms (accessible at https://forms.gle/nfuQuyPvhWgLqWnR8), facilitating broader access to respondents across diverse regions of Indonesia.

2.3 Sample size and data coding

Respondents were selected from three categories of MSMEs (micro, small, and medium enterprises). The sample size was determined by voluntary participation, and responses were coded for analysis. In total, the data were categorized into twelve distinct groups (A1-A12) based on key themes from previous research [14, 15]. This coding system enabled a structured analysis of responses.

2.4 Data analysis

After data collection, responses were edited and coded into categories for ease of analysis. The research employs descriptive statistical methods to analyze the data. Descriptive statistics, such as frequency distributions, measures of central tendency (mean, median, mode), and variability (standard deviation), are used to summarize and describe the data, offering insights into the level of awareness among MSMEs. While descriptive statistics do not provide causal relationships, they are effective in highlighting trends and general patterns in the data [22]. This study's analysis focuses on identifying the extent of MSMEs' awareness regarding personal data protection laws and standards. The alignment between different data protection frameworks (GDPR, PDP Law, and ISO/IEC 27001:2013) is further analyzed, Table 1 to provide a comprehensive understanding of how these frameworks intersect and influence MSMEs' practices.

3. RESULT AND DISCUSSION

3.1 Respondent demographics

The questionnaire was conducting from 10 May to 14 July 2023. The results of the distribution obtained 126 respondents who agreed to contribute. It shows in details on Table 4 shows the business location, the business type represents in Table 5, and Table 6 refers the business field of respondents.

Table 4. Business place MSMEs respondents

No.	Business Place (Province)	Total
1	Bali (Capital City Denpasar)	1
2	Banten (Capital City Serang)	7
3	D. I. Yogyakarta (Capital City Yogyakarta)	1
4	DKI Jakarta (Capital City Jakarta)	41
5	Jawa Barat (Capital City Bandung)	36
6	Jawa Tengah (Capital City Semarang)	15
7	Jawa Timur (Capital City Surabaya)	12
8	Kalimantan Barat (Capital City Pontianak)	2
9	Kalimantan Timur (Capital City Samarinda)	1
10	N. A. Darussalam (Capital City Banda Aceh)	2
11	Nusa Tenggara Timur (Capital City Kupang)	1
12	Riau (Capital City Pekanbaru)	1
13	Sulawesi Selatan (Capital City Makassar)	1
14	Sumatera Selatan (Capital City Palembang)	4
15	Sumatera Utara (Capital City Medan)	1

Table 5. Business type MSMEs respondents

No.	Business Type	Total	Percentage
1	Micro Business	59	46.8%
2	Small Business	28	22.2%
3	Medium Business	39	31%

Table 6. Business field MSMEs respondents

No.	Business Field	Total	Percentage
1	Souvenirs and Handicrafts	3	2.4%
2	Transportation	3	2.4%
3	Agribusiness	4	3.2%
4	Expedition	4	3.2%
5	Tourist	4	3.2%
6	Cosmetics	4	3.2%
7	Automotive	5	4%
8	Education	11	8.7%
9	Service	14	11.1%
10	Clothes	15	11.9%
11	Food and Drink	31	24.6%
12	Other	28	22.2%

3.2 Reliability and validity measurement

Determining reliability and validity is vital for assuring data replicability and accuracy [23]. In terms of reliability, the author uses alpha Cronbach coefficient and r value to evaluate the validity of the survey instrument [24].

The reliability examination was performed using alpha Cronbach coefficient, a reliability coefficient and a measure of internal consistency [25]. The formula alpha Cronbach coefficient is Eq. (1), number of questions is labelled by n. Furthermore, Vi refers to the variance of the score and V test refers to the total variances of the final score [26]. Acceptable values are above 0.70 [25]. The reliability measurement results are shown in Table 2 and for this study range between 0.947-0.953 and above the acceptance value.

$$\text{alpha Cronbach coefficient} = \frac{n}{n-1}\left(1 - \frac{\Sigma V1}{Vtest}\right) \qquad (1)$$

In assessing validity, Pearson's correlation coefficient as a consistency indicator is used to analyze the significant correlation between variables in the awareness instrument [27]. It was calculated by the formula Eq. (2). The Pearson correlation formula of two variables is by adding the differences of means and dividing the result by the differences of squared means [28].

$$r_{value} = \frac{\Sigma(\mathcal{X}_i - \overline{\mathcal{X}})(y_i - \overline{y})}{\sqrt{\Sigma(\mathcal{X}_i - \overline{\mathcal{X}})^2}\sqrt{\Sigma(y_i - \overline{y})^2}} \qquad (2)$$

The value of the r table for 126 respondents is above the r - value limit is detailed in Table 3, which is a significant level of 0.01 is 0.2287, and a significant level of 0.05 is 0.1750. It indicates that a significant correlation level between the question variables is valid. The reliability and validity of measurement results indicate that this research instrument is a reliable and valid measurement model. This study measures validity and reliability using IBM SPSS 27 as a tool.

3.3 Result

The survey was done using a valid instrument and a population sample based on measurement results that had been used with the same sample as this survey (Figure 1). Furthermore, the research result is in Table 7 as reference topic and item are from previous research [14, 15]. The study's findings are presented in detail, focusing on each critical topic concerning MSMEs' awareness of the PDP Law. The survey findings for each topic are explained below:

3.3.1 Knowledge of the law

The average score of 3.13 (SD = 1.35) for knowledge of the PDP Law indicates that legal awareness is moderately low across respondents. When compared with other key performance indicators, this score is among the lowest, highlighting a critical gap in foundational understanding of data protection laws. In comparison, consent management (mean = 3.49, SD = 1.24) and data security during processing (mean = 3.28, SD = 1.30) show relatively higher averages, suggesting that while businesses may engage in basic compliance activities, they often lack deeper legal knowledge. This disparity underscores the need for targeted legal education and awareness programs to bring law-related knowledge up to par with operational practices like data processing.

3.3.2 Consent from data owners

The consent management score of 3.49 (SD = 1.24) is slightly above average and indicates that businesses are somewhat consistent in obtaining consent from data owners. This score compares favorably against knowledge of the law (mean = 3.13) but falls short of the higher scores seen in data processing fundamentals (mean = 3.71, SD = 1.19). The relatively lower standard deviation in consent management suggests less variability, meaning that while consent procedures are more uniformly applied, there is still room for improvement, particularly in ensuring informed and explicit consent, as per GDPR and ISO/IEC 27001 standards.

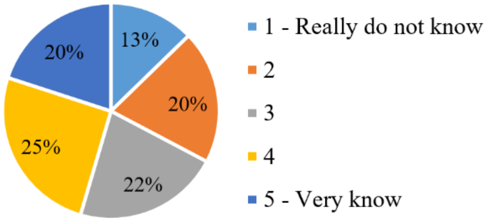

Figure 1. MSMEs Know PDP Law No. 27 of 2022

3.3.3 Data processing fundamentals

The data processing fundamentals score (mean = 3.71, SD = 1.19) is one of the highest among all indicators, signaling that MSMEs are more comfortable with the operational aspects of handling personal data. This high score contrasts sharply with the much lower score for written contracts with third parties (mean = 2.67, SD = 1.40), suggesting that while businesses may handle internal data processes well, they often fail to secure external relationships properly. This points to a potential vulnerability in data protection frameworks, where external third-party interactions are not given the same priority as internal operations.

3.3.4 Records of processing actions

With an average score of 3.00 (SD = 1.42) for logging and event tracking, this result is relatively low compared to other operational indicators like data security (mean = 3.28). This gap highlights a weakness in maintaining detailed records of data processing activities, which are essential for auditing and incident response under ISO/IEC 27001 Annex A.12.4.1 and A.12.4.3. A higher standard deviation (SD = 1.42) indicates more variability in compliance levels, with some businesses potentially lagging far behind in this area. Strengthening event logging systems could improve overall data protection and incident response capabilities.

Table 7. Descriptive statistic on awareness of Indonesian MSMEs with the PDP Law
(N = 126; 1 = Strongly Disagree to 5 = Strongly Agree)

Topic [14, 15]			Item [8, 14, 15, 19-21]	Mean	SD
Knowledge of law	A1	V1	We know the Personal Data Protection Law 2022, Number 27 occurred on 17 October 2022 in Indonesia.	3.13	1.35
Consent from data owner	A2	V1	The company or place of business has official consent from all personal data owners.	3.49	1.24
Processing fundamental	A3	V3	The company or place of business collects personal data that is necessary.	3.71	1.19
Record of processing action	A4	V4	The company or place of business has a surveillance camera (CCTV) to secure personal data.	3.00	1.42
		V5	The company or place of business has records of people accessing personal data.	3.02	1.39
Workforce law	A5	V6	The company or place of business has rules for using communication devices.	3.06	1.31
		V7	The company or place of business has socialized the rules for using communication tools.	3.08	1.31
Authority of the data owner	A6	V8	The company or place of business has records of activities carried out on personal data (data updating and data deletion).	3.10	1.39
		V9	The company or place of business informs the owner of the personal data about the length of time the personal data is stored.	2.81	1.30
		V10	The company or place of business provides access to personal data owners to complete and update data.	3.13	1.42
DPO	A7	V11	The company or place of business appoints a special officer to manage stored personal data.	2.98	1.32
Secureness of processing data	A8	V12	The company or place of business has a mechanism to ensure their information is secured	3.28	1.30
Written Contracts	A9	V13	The company or place of business cooperates with third parties in using personal data.	2.67	1.40
		V14	The company or place of business has a written agreement to ensure their information is secured	2.99	1.35
Pass on the personal data to other countries	A10	V15	The company or place of business exchanges personal data abroad.	2.25	1.28
		V16	The company or place of business exchanges personal data with a destination country with higher rules and is legal (for example EU).	2.17	1.23
		V17	The company or place of business has written approval for exchanging data abroad.	2.39	1.26
Obedience of data regulator	A11	V18	The company or place of business regularly assesses compliance with laws and regulations of personal data protection.	3.02	1.26
Disclosure to the officials about the breach of private data	A12	V19	The company or place of business informs a data security breach that has occurred.	3.05	1.28
		V20	The company or place of business has a record of a data security breach that occurred.	2.64	1.35

3.3.5 Workforce law

The score for workforce-related rules (mean = 3.06, SD = 1.31) reveals moderate compliance with employee awareness of communication device policies and security protocols. This indicator shows some alignment with data security (mean = 3.28), but the moderate scores suggest that workforce compliance programs are not fully effective. The high variability (SD = 1.31) implies inconsistent application of workforce security policies, which could expose businesses to higher risks of data breaches. This further emphasizes the need for continuous security training and a more structured approach to enforcing policies across the workforce.

3.3.6 Data owner rights

The score of 3.10 (SD = 1.39) for managing personal data records shows that businesses are moderately compliant with the rights of data owners. This score sits between consent management (mean = 3.49) and cross-border data transfers (mean = 2.17), indicating that while businesses pay some attention to data owner rights, cross-border transfers pose significant challenges. The lower mean score for informing data owners about retention periods (2.81, SD = 1.30) suggests that transparency and communication are weak points in data governance, pointing to areas for improvement in how companies handle the rights of data subjects.

3.3.7 Data protection officer (DPO)

The relatively low score of 2.98 (SD = 1.32) for appointing a Data Protection Officer (DPO) indicates that most MSMEs have not yet complied with this critical requirement. This low average, when compared with operational metrics like data processing (mean = 3.71), reveals a significant gap in governance structures. The lack of a designated DPO weakens the organization’s ability to manage data protection programs effectively and monitor compliance, highlighting an urgent need for businesses to appoint a DPO as mandated by the PDP Law and ISO/IEC 27001 Annex A.6.1.1.

3.3.8 Data security during processing

The mean score of 3.28 (SD = 1.30) for securing data during processing shows a moderate level of adherence to security controls. This score is higher than knowledge of the law (mean = 3.13) but lower than data processing fundamentals (mean = 3.71), indicating that while operational security measures are somewhat implemented, there is still room for strengthening these protocols, especially given the rapid evolution of cyber threats. Reducing variability (SD = 1.30) through standardized processes would ensure more consistent protection of personal data during processing.

3.3.9 Written contracts

The mean score of 2.67 (SD = 1.40) for securing third-party agreements through written contracts is one of the lowest among all performance indicators, highlighting a critical vulnerability in external data governance. When compared with internal data processing scores (mean = 3.71), the sharp contrast points to a significant oversight in managing external risks. Businesses must prioritize third-party risk management by formalizing agreements that clearly outline data protection obligations as required by both the PDP Law and ISO/IEC 27001 Annex A.15.1.2.

3.3.10 Cross-border data transfers

The low score for cross-border data transfers (mean = 2.25; SD = 1.28) indicates that only 22 of the respondents' companies exchange data abroad. The majority of businesses have not yet engaged in international data use. According to the questionnaire results, the companies that share data abroad already have written consent to use the data owner's information. The low scores (ranging from 2.17 to 2.39) do not indicate a significant deficiency in compliance with the ISO/IEC 27001:2013 standard for managing international data transfers. However, of the 22 companies that do exchange personal data across borders, some already follow proper policies and approvals, while the rest have not yet engaged in international data exchange.

3.3.11 Regulatory compliance

The mean score of 3.02 (SD = 1.26) for regulatory compliance suggests that many businesses are moderately aligned with legal requirements but fail to maintain continuous compliance monitoring. When compared to other performance indicators, such as data processing (mean = 3.71), the lower score for regulatory compliance points to the need for more frequent and comprehensive audits, as mandated by ISO/IEC 27001 Annex A.18.2.3. Implementing continuous monitoring and regular audits will help businesses identify and address compliance gaps more effectively.

3.3.12 Data breach notifications

The mean score of 3.05 (SD = 1.28) for data breach notifications highlights moderate compliance with breach reporting requirements. However, the low score of 2.64 (SD = 1.35) for maintaining records of data breaches reveals significant weaknesses in the documentation and tracking of incidents, which are essential for compliance with PDP Law Article 46. Businesses must develop formal processes for breach reporting and documentation to enhance their incident response capabilities and mitigate the impact of security breaches.

3.3.13 Quantitative comparison conclusion

The analysis of various performance indicators reveals notable disparities in the awareness and compliance levels of Indonesian MSMEs regarding data protection practices. The moderately low score for knowledge of the PDP Law (mean = 3.13, SD = 1.35) underscores a significant gap in legal awareness, which is crucial for comprehensive data protection. In contrast, consent management (mean = 3.49, SD = 1.24) and data processing fundamentals (mean = 3.71, SD = 1.19) show relatively higher scores, indicating that businesses are somewhat consistent in obtaining consent and managing data processing activities.

However, significant weaknesses are evident in third-party agreements (mean = 2.67, SD = 1.40), reflecting critical areas where MSMEs are vulnerable. These low scores suggest a pressing need for better contractual safeguards. Additionally, the low appointment rate of Data Protection Officers (mean = 2.98, SD = 1.32) highlights a governance gap that could undermine overall data protection efforts. To address these deficiencies, MSMEs must invest in targeted legal education and awareness programs, enhance their data processing and security measures, formalize data processing agreements, and appoint dedicated Data Protection Officers. These steps are essential to foster a culture of data protection and ensure long-term business sustainability in the digital economy.

These disparities suggest that while MSMEs may have implemented some internal data protection measures, they face considerable challenges in governance, external risk management, and legal compliance. Addressing these gaps will require a concerted effort to enhance legal awareness, formalize third-party contracts, and ensure proper governance structures are in place, such as appointing a DPO and establishing cross-border data transfer safeguards.

3.4 Discussion

This study identified 12 critical areas based on earlier research [14, 15] to assess the awareness of Indonesian MSMEs regarding personal data protection, focusing on compliance with Indonesia's Personal Data Protection (PDP) Law [8, 19, 20], and its alignment with ISO/IEC 27001:2013 standards [28]. The findings revealed that the awareness and practices of Indonesian MSMEs in this area remain relatively low, with significant gaps in compliance, particularly in terms of understanding and implementing key legal and data protection requirements.

When compared with the implementation of the General Data Protection Regulation (GDPR) in Europe, this study's findings echo similar challenges. Studies on European SMEs show a persistent lack of awareness of GDPR obligations, which remains a common issue in non-compliance cases [29, 30]. Likewise, the Indonesian MSMEs in this study exhibited a limited understanding of PDP Law, leading to non-compliance with critical provisions, such as obtaining explicit consent from data owners (A2) and ensuring secure third-party data processing agreements (A9). Similar issues have been observed in Europe, where SMEs reported difficulties in interpreting and implementing GDPR due to a lack of clear guidance and limited resources [31].

The disparity between MSMEs’ awareness of local regulations (PDP Law) and international standards (ISO/IEC 27001:2013) highlights a broader global trend where small and medium-sized enterprises (SMEs) struggle to meet stringent data protection requirements. Previous research has noted that European SMEs also encountered challenges in complying with GDPR because of their lack of in-house expertise and the high costs associated with implementing robust data protection frameworks [32]. Similarly, the Indonesian MSMEs surveyed in this study lack dedicated personnel, such as Data Protection Officers (DPOs), who are essential for managing data protection and ensuring compliance with both local and international standards (A7). This issue is not unique to Indonesia, as studies have shown that SMEs across different regions often face similar challenges in appointing DPOs and establishing strong governance structures for data protection

[33].

A critical comparison can be drawn with ISO/IEC 27001's role in supporting GDPR compliance in Europe. Research has demonstrated that ISO 27001 helps organizations maintain a consistent Information Security Management System (ISMS), which aligns with GDPR's emphasis on reducing the risk of data breaches [21]. The findings of this study indicate that Indonesian MSMEs have similar deficiencies in their information security practices, as demonstrated by their low scores in maintaining secure data processing environments and establishing formal third-party agreements (A8, A9). These challenges suggest that Indonesian MSMEs, like their European counterparts, need to integrate ISO/IEC 27001:2013 controls more comprehensively into their operations to meet PDP Law requirements and reduce their vulnerability to data breaches.

Additionally, studies in the European context have highlighted that one of the most frequent issues with GDPR compliance is a lack of awareness and preparedness regarding information security [21].This study's findings are consistent with this observation, as MSMEs in Indonesia also display significant gaps in understanding the importance of compliance with both PDP Law and ISO/IEC 27001:2013, particularly in areas such as data breach notification (A12) and secure handling of cross-border data transfers (A10). The low awareness of these critical aspects puts MSMEs at a higher risk of non-compliance, potentially leading to legal penalties and reputational damage.

It is worth noting that while GDPR compliance is mandatory for businesses operating within or interacting with the European Union, the PDP Law in Indonesia is still relatively new, and awareness efforts are only beginning to take shape. As seen in Europe, it is likely that as enforcement actions increase and awareness campaigns gain momentum, MSMEs in Indonesia will face similar pressures to comply with the PDP Law. The lack of preparedness among Indonesian MSMEs, as revealed by this study, mirrors the early stages of GDPR implementation, where many businesses were slow to adapt to the new regulations.

3.4.1 Geographical context and global comparisons

In contrast to European SMEs, where GDPR enforcement has been in place for several years, Indonesian MSMEs are still in the initial phases of adapting to the PDP Law. However, the challenges observed in Indonesia may also reflect those faced by SMEs in other emerging markets where data protection regulations are relatively new or less stringently enforced. For instance, studies from other regions, such as Africa and Southeast Asia, also show that SMEs struggle with compliance due to a lack of resources, expertise, and regulatory support [33]. In many developing countries, regulatory frameworks are still evolving, and businesses often prioritize immediate operational needs over compliance with data protection laws.

In the global context, the findings of this study underscore the universal challenges faced by SMEs in balancing compliance with legal standards and operational efficiency. As more countries adopt stringent data protection laws modeled after GDPR, such as the Brazilian General Data Protection Law (LGPD) or the PDP Law in Indonesia, the issues of awareness, expertise, and resource constraints will likely persist. This calls for more targeted support from regulatory bodies, including providing clearer guidance and resources tailored to the needs of SMEs.

3.4.2 Recommendations for improving compliance

Based on the findings of this study, several recommendations can be made to help Indonesian MSMEs improve their compliance with the PDP Law and ISO/IEC 27001:2013. First, it is essential for MSMEs to conduct regular training sessions and awareness programs to ensure employees, especially those involved in data processing, are knowledgeable about legal requirements and the importance of data protection. This is consistent with the approach taken by European SMEs, where training programs have been shown to improve compliance rates [31].

Additionally, MSMEs must develop standardized procedures for obtaining explicit consent from data owners and ensure that personal data is collected only for legitimate business purposes. This will not only improve compliance with PDP Law requirements but also build trust with customers, which is crucial for long-term business success. Regular internal audits and assessments, as recommended by ISO/IEC 27001:2013, should also be implemented to monitor ongoing compliance and identify areas for improvement.

Finally, MSMEs should formalize their relationships with third-party service providers by ensuring that data processing agreements are in place, as required by both PDP Law and ISO/IEC 27001:2013. This will help mitigate the risks associated with outsourcing data processing activities and ensure that personal data is handled securely throughout the supply chain.

4. CONCLUSIONS

This study highlights critical areas where Indonesian MSMEs need to enhance their compliance with the Personal Data Protection (PDP) Law and ISO/IEC 27001:2013 standards. The relatively low awareness of the PDP Law (mean = 3.13) underscores the necessity for targeted legal education and awareness campaigns. Although consent management practices showed moderate compliance (mean = 3.49), they require more consistent procedures to fully meet legal standards.

Operational strengths were noted in data processing fundamentals (mean = 3.71), yet significant weaknesses in third-party agreements (mean = 2.67) and cross-border data transfers (mean = 2.17) highlight vulnerabilities in managing external data risks. The low appointment rate of Data Protection Officers (mean = 2.98) indicates a critical governance gap. Moderate scores in data breach notifications (mean = 3.05) and incident tracking (mean = 2.64) further emphasize the need for improved compliance mechanisms.

Future research should focus on developing effective training programs to improve knowledge of PDP Law and ISO/IEC 27001:2013 standards, formalizing data processing agreements, appointing dedicated Data Protection Officers, and implementing continuous compliance audits. Addressing these challenges is vital for fostering a culture of data protection and ensuring sustainable business practices in the digital economy.

ACKNOWLEDGMENT

This work was supported by the Research Grant Faculty of Computer Science, University of Indonesia, 2024, Number NKB-1/UN2.F11.D/HKP.05.00/2024.

REFERENCES

[1] Fuciu, M., Dragomir, A.N. (2021). Changes in the buying behaviour of the companies within the context of the digital environment. Scientific Bulletin, 26(2): 138-147. http://doi.org/10.2478/bsaft-2021-0016

[2] Hashmi, S.S., Mohammad, A.A.K., Abdul, A.M., Atheeq, C., Nizamuddin, M.K. (2024). Enhancing data security in multi-cloud environments: A Product Cipher-Based Distributed Steganography approach. International Journal of Safety and Security Engineering, 14(1): 47-61. https://doi.org/10.18280/ijsse.140105

[3] Nelakuditi, N.C., Namburi, N.K., Sayyad, J., Rudraraju, D.V, Govindan, R., Rao, P.V. (2024). Secure file operations: Using advanced encryption standard for strong data protection. International Journal of Safety & Security Engineering, 14(3): 1007-1014. https://doi.org/10.18280/ijsse.140330

[4] Zywiołek, J., Trigo, A., Rosak-Szyrocka, J., Khan, M.A. (2022). Security and privacy of customer data as an element creating the image of the company. Management Systems in Production Engineering, 30(2): 156-162. https://doi.org/10.2478/mspe-2022-0019

[5] Amirulbahar, A., Ruldeviyani, Y. (2023). Analysis of effects of app permission concerns on intentions to disclose personal information: A case study of money transfer service app. Jurnal Ilmu Pengetahuan dan Teknologi Komputer, 9(1): 109-118. http://doi.org/10.33480/jitk.v9i1.4316

[6] Goel, A., Prabha, C., Malik, M., Sharma, P. (2024). Security concerns and data breaches for data deduplication techniques in cloud storage: A brief meta-analysis. International Journal of Safety and Security Engineering, 14(2): 435-446. https://doi.org/10.18280/ijsse.140211

[7] Cisco Secure, "Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense," Cisco, 2021. https://www.cisco.com/c/dam/global/en_sg/products/security/meet-max-report-2021/assets/data/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf.

[8] Sudarwanto, A.S., Kharisma, D.B.B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. Journal of Financial Crime, 29(4): 1443-1457. https://doi.org/10.1108/JFC-09-2021-0193

[9] Strzelecki, A., Rizun, M. (2020). Consumers' security and trust for online shopping after GDPR: Examples from Poland and Ukraine. Digital Policy, Regulation and Governance, 22(4): 289-305. http://doi.org/10.1108/DPRG-06-2019-0044

[10] Shakti, F.N., Hidayanto, A.N. (2024). Measurement of employee information security awareness: Case study at financial institution. Jurnal Ilmu Pengetahuan dan Teknologi Komputer, 9(2): 172-179. http://doi.org/10.33480/jitk.v9i2.4163

[11] Buckley, G., Caulfield, T., Becker, I. (2022). 'It may be a pain in the backside but...' insights into the resilience of business after GDPR. In Proceedings of the 2022 New Security Paradigms Workshop, pp. 21-34. http://doi.org/10.1145/3584318.3584320

[12] Leite, L., dos Santos, D.R., Almeida, F. (2022). The impact of general data protection regulation on software engineering practices. Information and Computer Security, 30(1): 79-96. http://doi.org/10.1108/ICS-03-2020-0043

[13] Bharti, S.S., Aryal, S.K. (2023). The right to privacy and an implication of the EU General Data Protection Regulation (GDPR) in Europe: Challenges to the companies. Journal of Contemporary European Studies, 31(4): 1391-1402. http://doi.org/10.1080/14782804.2022.2130193

[14] da Conceição Freitas, M., da Silva, M.M. (2022). GDPR and suppliers in SMEs. In 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 1-6. http://doi.org/10.23919/CISTI54924.2022.9820586

[15] da Conceição Freitas, M., da Silva, M.M. (2018). GDPR Compliance in SMEs: There is much to be done. Journal of Information Systems Engineering & Management, 3(4): 30. http://doi.org/10.20897/jisem/3941

[16] Barlette, Y., Fomin, V.V. (2008). Exploring the suitability of IS security management standards for SMEs. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, HI, USA, p. 308. http://doi.org/10.1109/HICSS.2008.167

[17] Taşkın, G., Sandıkkaya, M.T. (2023). Comparison of security frameworks for SMEs. In 14th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkiye, pp. 1-5. https://doi.org/10.1109/ELECO60389.2023.10416030

[18] Antunes, M., Maximiano, M., Gomes, R., Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2): 219-238. http://doi.org/10.3390/jcp1020012

[19] Mayulu, H., Topan, E.A., Haris, M.I., Daru, T.P. (2021). The personal data protection of internet users in Indonesia. Journal of Southwest Jiaotong University, 56(1): 164-175. https://doi.org/10.35741/issn.0258-2724.56.1.15

[20] Indonesia, Pemerintah Pusat. Undang-undang (UU) Nomor 27 Tahun 2022. LN.2022/No.196, TLN No.6820, jdih.setneg.go.id. Available: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022, accessed on Oct. 15, 2024.

[21] Suorsa, M., Helo, P. (2023). Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis. Information Security Journal: A Global Perspective, 33(3): 285-306. http://doi.org/10.1080/19393555.2023.2270984

[22] Baker, K., Burd, L., Figueroa, R. (2024). Consumer nutrition environment measurements for nutrient-dense food availability and food sustainability: A scoping review. Archives of Public Health, 82(1): 7. http://doi.org/10.1186/s13690-023-01231-y

[23] Koech, A.K., Buyle, S., Macário, R. (2023). Airline brand awareness and perceived quality effect on the attitudes towards frequent-flyer programs and airline brand choice—Moderating effect of frequent-flyer programs. Journal of Air Transport Management, 107: 102342. http://doi.org/10.1016/j.jairtraman.2022.102342

[24] Taghizadeh, G., Sarlak, N., Fallah, S., Sharabiani, P.T.A., Cheraghifard, M. (2024). Minimal clinically important difference of fatigue severity scale in patients with

chronic stroke. Journal of Stroke and Cerebrovascular Diseases, 33(4): 107577. https://doi.org/10.1016/j.jstrokecerebrovasdis.2024.107577

[25] Rosli, M.S., Saleh, N.S., Alshammari, S.H., Ibrahim, M.M., Atan, A.S., Atan, N.A. (2021). Improving Questionnaire Reliability using Construct Reliability for researches in educational technology. International Journal of Interactive Mobile Technologies, 15(4): 109-116. https://doi.org/10.3991/ijim.v15i04.20199

[26] Li, S.J., Wu, H.W., Wang, Y.S. (2024). Positive emotions, self-regulatory capacity, and EFL performance in the Chinese senior high school context. Acta Psychologica, 243: 104143. http://doi.org/10.1016/j.actpsy.2024.104143

[27] Berman, J.J. (2016). Data Simplification: Taming Information with Open Source Tools. Morgan Kaufmann Publishers Inc., San Francisco, CA, United States. https://dl.acm.org/doi/book/10.5555/3044785

[28] Suorsa, M., Helo, P. (2023). Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis. Information Security Journal: A Global Perspective, 33(3): 285-306. http://doi.org/10.1080/19393555.2023.2270984

[29] Mangini, V., Tal, I., Moldovan, A.N. (2020). An empirical study on the impact of GDPR and right to be forgotten—Organisations and users perspective. In Proceedings of the 15th International Conference on Availability, Reliability and Security, New York, NY, USA: ACM, pp. 1-9. http://doi.org/10.1145/3407023.3407080

[30] Pathak, P., Pal, P.R., Maurya, R.K., Rishabh, Rahul, M., Yadav, V. (2023). Assessment of compliance of GDPR in IT industry and fintech. Lecture Notes in Networks and Systems, 421: 703-713. http://doi.org/10.1007/978-981-19-1142-2_55

[31] Smirnova, Y., Travieso-Morales, V. (2024). Understanding challenges of GDPR implementation in business enterprises: A systematic literature review. International Journal of Law and Management, 66(3): 326-344. http://doi.org/10.1108/IJLMA-08-2023-0170

[32] Almeida Teixeira, G., Mira da Silva, M., Pereira, R. (2019). The critical success factors of GDPR implementation: A systematic literature review. Digital Policy, Regulation and Governance, 21(4): 402-418. http://doi.org/10.1108/DPRG-01-2019-0007

[33] Härting, R.C., Kaim, R., Klamm, N., Kroneberg, J. (2021). Impacts of the new general data protection regulation for small- and medium-sized enterprises. Advances in Intelligent Systems and Computing, 1183: 238-246. http://doi.org/10.1007/978-981-15-5856-6_23