



Safeguarding Consumer Data in the Digital Age: Security and Protection in the E-Commerce Ecosystem

BY

Derah Sudjaniah¹, Yustinus Rawi Dandono², Bintoro Ariyanto³, Melva Arita⁴, Yusuf Budi Harto⁵

^{1,2,3,4,5} Sekolah Tinggi Ilmu Ekonomi Bhakti Pembangunan



Article History

Received: 10/09/2026

Accepted: 17/09/2026

Published: 21/09/2026

Vol – 2 Issue – 9

PP: -74-82

Abstract

This study aims to analyze the influence of consumer data security, regulatory compliance, and privacy policy transparency on purchase decisions in e-commerce, with consumer trust as a moderating variable. Data were collected through a survey of 394 digital platform users and analyzed using Structural Equation Modeling with the Partial Least Squares approach via SmartPLS. The results show that all three independent variables positively influence purchase decisions, with privacy policy transparency exerting the strongest impact on consumer perception. Consumer trust significantly moderates the relationships, amplifying the effects of data security, regulatory compliance, and transparency on buying behavior. The findings emphasize that comprehensive data protection practices are not only legal obligations but also strategic tools to foster trust, enhance customer loyalty, and drive purchasing decisions in the digital era.

Keywords: Data Security, Regulatory Compliance, Privacy Transparency, Consumer Trust, Purchase Decision, Business Digital.

INTRODUCTION

With increasing digitalization, e-commerce has become an integral part of daily life for people around the world, including in Indonesia. The rapid growth of this sector is driven by the dominance of millennial and Generation Z consumers who are highly familiar with technology (Kredivo & Katadata, 2023). However, along with the rise in online transactions, concerns have emerged regarding the inadequate protection of consumers' personal data. Cases of data breaches and the misuse of personal information are becoming increasingly frequent, raising questions about how secure consumer data is during online transactions (BPKN-RI, 2023).

In Indonesia, although regulations for personal data protection already exist, their effectiveness remains limited due to various challenges. Several issues have been identified, including unmonitored financial transactions, e-commerce fraud, transaction security concerns, and personal data vulnerabilities (BPKN-RI, 2023). This situation has raised consumer concerns regarding the safety of their data when conducting online transactions. Recent reports from the National Consumer Protection Agency (BPKN) in 2024 indicate that throughout that year, BPKN received 1,733 complaints across various sectors, with total potential consumer losses reaching IDR 424.2 billion, and recovered losses amounting to IDR 44.8 billion (BPKN-RI, 2024). By

February 2025, BPKN had also received 500 reports related to Korean music event arrangements, with estimated losses reaching IDR 6 billion (20.detik.com, 2025). These figures indicate that consumer protection issues, including in the e-commerce sector, remain a major concern for BPKN.

Previous studies have highlighted the importance of data security in influencing consumer purchase decisions. For instance, research by Sihombing et al. (2024) found that challenges in implementing consumer protection regulations in e-commerce remain a significant issue. In addition, other studies suggest that regulatory compliance plays a role in enhancing consumer trust in digital transactions (Sri Lestari Poernomo, 2023). Meanwhile, research by Chaniago et al. (2025) highlights weaknesses in data security on the Shopee e-commerce platform, but does not specifically link security factors to consumer purchase decisions. Another study by Maharani & Prakoso (2024) found that regulations related to personal data protection are still not fully effective in protecting consumers from potential security breaches. Furthermore, Humaira (2024) identified challenges in e-commerce users' personal data security, but did not examine its direct effect on purchase decisions. This research gap indicates that relatively few studies have explicitly analyzed the impact of data security, regulatory compliance, and privacy policy transparency on purchase decisions, as well as how consumer trust moderates these relationships.

*Corresponding Author: Derah Sudjaniah..



This study is grounded in two theoretical perspectives. First, the Theory of Planned Behavior (TPB) by Ajzen (1991), which states that individual behavior is influenced by attitudes, subjective norms, and perceived behavioral control. In this context, perceptions of data security and privacy policy transparency shape consumers' attitudes toward purchase decisions. Second, Trust-Based Theory explains that trust is a key element in the relationship between consumers and digital service providers. Trust functions as a risk reducer and strengthens the influence of positive perceptions on purchase decisions (Morgan, 2015; Garbarino, 2014).

Based on these perspectives, this study focuses on evaluating the impact of consumer data security, regulatory compliance, and privacy policy transparency on e-commerce purchase decisions, with consumer trust as a moderating variable. This research is expected to contribute theoretically to the e-commerce literature and provide practical implications for digital business actors and policymakers in building a secure and trustworthy transaction ecosystem.

The urgency of this research lies in the need to understand how data security, regulatory compliance, and privacy policy transparency influence consumer purchase decisions, as well as how consumer trust moderates these relationships. With the increasing number of data breaches and rising consumer concerns, this study is expected to contribute to the development of more effective and secure digital marketing strategies.

The focus of this research is to explore the influence of consumer data security, regulatory compliance, and privacy policy transparency on purchase decisions, while considering consumer trust as a moderating variable. The aim is to identify key factors that affect purchasing decisions in the e-commerce context, thereby providing recommendations for digital business practitioners to enhance consumer trust and loyalty.

Research Elaboration

Based on the literature review presented, this study emphasizes that consumer data security, regulatory compliance, and privacy policy transparency are critical factors in shaping consumer purchase decisions in e-commerce platforms. Consumer data security is a crucial element because it is directly related to the protection of users' personal information, encompassing both technical aspects such as encryption and authentication, as well as legal safeguards. Research by Zahwani et al. (2023) indicates that legal protection of personal data in e-commerce transactions plays an important role in preventing cybercrime and enhancing consumer perceptions of safety.

Regulatory compliance, particularly with data protection frameworks such as Law No. 27 of 2022 on Personal Data Protection, which became fully effective on October 17, 2024, serves as a fundamental legal foundation for managing digital data in Indonesia (indonesia.go.id, 2024). This regulation not only functions as a legal obligation but also as a credibility signal that enhances consumer trust in digital platforms.

Previous research by Sri Lestari Poernomo (2023) also confirms that regulatory compliance contributes significantly to increasing consumer trust in digital transactions.

Privacy policy transparency is another essential factor, as it enables consumers to understand how their personal data is collected, processed, and protected. Aziz (2022) states that transparency in privacy policies can reduce consumer concerns regarding data misuse while increasing comfort and purchase intention on e-commerce platforms. Furthermore, in the context of digital marketing strategy, the implementation of regulations such as the General Data Protection Regulation (GDPR) has significant implications. Hermansyah & Astini (2024) emphasize that compliance with data protection regulations not only reduces legal risks but also enhances brand trust and corporate reputation.

This study employs a quantitative research approach using a survey method as the primary data collection technique (Sujarweni, 2024; Rahmawan, 2023). The population consists of e-commerce users in Indonesia who have made at least one online purchase within the past year. Since the population is considered infinite, the sample size is determined using the Cochran formula (Sudarmanto, 2013):

$$n = \frac{z^2 p(1-p)}{e^2}$$

Where:

Z = 1.96 (95% confidence level),

p = 0.5,

e = 0.05

Calculation:

$$n_0 = \frac{(1,96)^2 \times 0,5 \times 0,5}{(0,05)^2}$$

$$n_0 = \frac{3,8416 \times 0,25}{0,0025}$$

$$n_0 = \frac{0,9604}{0,0025} = 384,16$$

Thus, the minimum required sample size is 384 respondents. In this study, 394 respondents were obtained, which exceeds the minimum requirement and ensures adequate statistical validity (Zulfikar, 2024). Data were collected through an online survey using Google Forms distributed to e-commerce users in Indonesia on March 23, 2025, using a random sampling technique due to the large and undefined population (Aiman et al., 2023).

The research instrument was measured using a 5-point Likert scale (Ardhini, 2023), covering consumer data security, regulatory compliance, privacy policy transparency, purchase decision, and consumer trust. Construct validity was assessed using outer loadings and Average Variance Extracted (AVE), while reliability was tested using Cronbach's Alpha and Composite Reliability (Widodo et al., 2023).

Data analysis was conducted using Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS 4 to examine the relationships among variables and the moderating effect of consumer trust (Setiabudhi et al., 2025). The analysis procedure included descriptive statistics, convergent validity testing (outer loading > 0.70; AVE > 0.50) (Binus University, 2021c), reliability testing (Cronbach's Alpha and Composite Reliability > 0.70) (Binus University, 2021a), and discriminant validity using HTMT (< 0.90) (Binus University, 2021b). In addition, R-square analysis was used to evaluate the explanatory power of the model (0.25 = weak, 0.50 = moderate, 0.75 = strong), along with model fit evaluation using SRMR, NFI, RMS_theta, and Goodness of Fit (GoF), calculated as $GoF = \sqrt{(AVE \times R^2)}$ (Rahadi, 2023; Tenenhaus et al., 2005). Effect size (f^2) was also assessed, and hypothesis testing was conducted using bootstrapping with 5,000 subsamples, where a p-value < 0.05 indicates statistical significance.

Theoretically, this study is grounded in the Theory of Planned Behavior (Ajzen, 1991), which explains that individual behavior is influenced by attitudes, subjective norms, and perceived behavioral control. In this context, perceptions of data security and privacy transparency shape consumer attitudes toward purchase decisions. Additionally, Trust-Based Theory (Morgan, 2015; Garbarino, 2014) posits that trust is a key mechanism for reducing uncertainty in digital transactions and strengthening the relationship between positive perceptions and purchasing behavior.

Therefore, consumer data security, regulatory compliance, and privacy policy transparency are positioned as key determinants of purchase decisions, while consumer trust functions as a moderating variable that strengthens these relationships. The higher the level of consumer trust in an e-commerce platform, the stronger the influence of these variables on purchase decisions. This study is expected to contribute both theoretically to the e-commerce literature and practically to digital business practitioners and policymakers in building a secure, transparent, and trustworthy digital ecosystem.

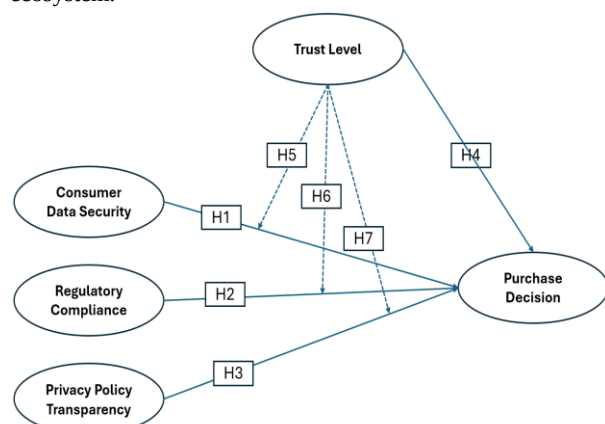


Figure 1. Research Framework

Results and Discussion

The demographic characteristics of the respondents in this study are presented to provide an overview of the sample based on several key criteria.

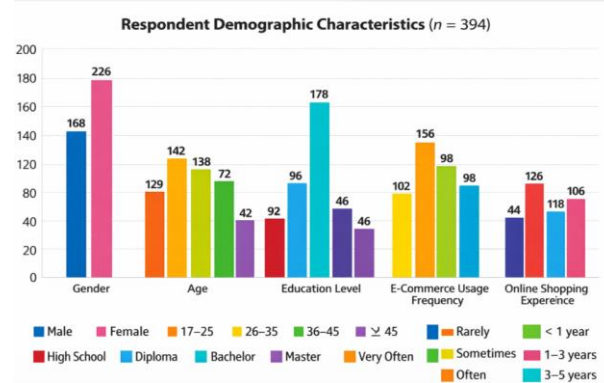


Figure 2. Demographic characteristics of the respondents
Source: Data Processing (2026)

Based on the respondent demographic chart (n = 394), the majority of respondents were female (226) compared to male (168). Most respondents were aged 17–25 years (142) and 26–35 years (138), followed by 36–45 years (72) and over 45 years (42). In terms of education, respondents were dominated by those with a bachelor's degree (178), followed by high school (96), diploma (74), and master's degree (46). Furthermore, most respondents reported using e-commerce frequently (156) and very frequently (98), while 102 respondents used it occasionally and 38 rarely used it. In terms of online shopping experience, 126 respondents had 1–3 years of experience, 118 had 3–5 years, 106 had more than 5 years, and 44 had less than 1 year. These characteristics indicate that respondents are active and experienced e-commerce users, making them relevant for analyzing the influence of consumer data security, regulatory compliance, and privacy policy transparency on purchase decisions, with trust level as a moderating variable.

1. Measurement Model Results (Outer Model)

The outer loading values were examined to assess the convergent validity of each indicator in measuring their respective constructs.

Table 1. Outer Loadings

Indicator	X1	X2	X3	Y	Z	Z × X1	Z × X2	Z × X3
X1.1	0.871							
X1.2	0.878							
X1.3	0.867							
X1.4	0.854							
X1.5	0.872							
X2.1		0.899						
X2.2		0.891						
X2.3		0.877						
X2.4		0.865						
X2.5		0.899						
X3.1			0.901					
X3.2			0.877					
X3.3			0.857					
X3.4			0.874					
X3.5			0.848					
Y1				0.876				
Y2				0.897				
Y3				0.865				
Y4				0.896				
Y5				0.880				
Z1					0.875			
Z2					0.864			
Z3					0.843			
Z4					0.894			
Z5					0.888			
Z × X1						1.000		
Z × X2							1.000	
Z × X3								1.000

Source: Data Processing (2026)

The outer loading values in the measurement model indicate that all indicators have loading factors above the recommended threshold of 0.70. The indicators for Consumer Data Security (X1) range from 0.854 to 0.878, Regulatory Compliance (X2) range from 0.865 to 0.899, and Privacy Policy Transparency (X3) range from 0.848 to 0.901. Furthermore, the Purchase Decision (Y) construct shows outer loading values between 0.865 and 0.897, while Trust Level (Z) ranges from 0.843 to 0.894. The interaction variables (Z × X1, Z × X2, and Z × X3) also show values of 1.000,

indicating strong moderating construct formation. These results demonstrate that all indicators used in this study have good convergent validity and are capable of measuring their respective constructs reliably. This means that the indicators successfully represent Consumer Data Security, Regulatory Compliance, and Privacy Policy Transparency in explaining Purchase Decisions. In addition, the Trust Level variable as a moderating variable is also well measured, indicating that trust plays an important role in strengthening the relationship between the independent variables and purchase decisions in e-commerce.

The construct reliability and validity were assessed to evaluate the internal consistency and convergent validity of each construct in the measurement model.

Table 2. Construct reliability and validity

Construct	Cronbach's Alpha	Composite Reliability (rho_a)	Composite Reliability (rho_c)	Average Variance Extracted (AVE)
Consumer Data Security (X1)	0.918	0.928	0.938	0.751
Regulatory Compliance (X2)	0.932	0.936	0.948	0.786
Privacy Policy Transparency (X3)	0.921	0.931	0.940	0.759
Purchase Decision (Y)	0.930	0.937	0.946	0.780
Trust Level (Z)	0.923	0.947	0.941	0.762

Source: Data Processing (2026)

The construct reliability and validity results indicate that all variables meet the recommended thresholds. The Cronbach's alpha values for all constructs range from 0.918 to 0.932, exceeding the minimum requirement of 0.70, which indicates strong internal consistency. Similarly, the composite reliability values (rho_a and rho_c) for all constructs are above 0.70, demonstrating that each construct has high reliability. Furthermore, the Average Variance Extracted (AVE) values range from 0.751 to 0.786, which are above the recommended threshold of 0.50. This indicates good

convergent validity, meaning that each construct explains more than 50% of the variance of its indicators. These findings confirm that Consumer Data Security, Regulatory Compliance, and Privacy Policy Transparency are reliable constructs in explaining Purchase Decision, while Trust Level is also valid and reliable as a moderating variable in the research model.

Discriminant validity was assessed to ensure that each construct is empirically distinct and captures phenomena not represented by other constructs in the model.

Table 3. Discriminant validity

Construct	X1	X2	X3	Y	Z	Z×X3	Z×X2	Z×X1
X1	—							
X2	0.039	—						
X3	0.044	0.028	—					
Y	0.212	0.224	0.247	—				
Z	0.054	0.060	0.072	0.172	—			
Z×X3	0.097	0.043	0.080	0.436	0.058	—		
Z×X2	0.070	0.061	0.042	0.147	0.071	0.122	—	
Z×X1	0.086	0.064	0.103	0.225	0.060	0.039	0.081	—

Source: Data Processing (2026)

The discriminant validity results based on the Heterotrait–Monotrait Ratio (HTMT) show that all values are below the recommended threshold of 0.90. The HTMT values between Consumer Data Security (X1), Regulatory Compliance (X2), and Privacy Policy Transparency (X3) are very low, indicating that each construct is empirically distinct. Furthermore, the HTMT values between the independent variables and Purchase Decision (Y) range from 0.212 to 0.247, while Trust Level (Z) shows values between 0.054 and 0.172, all below the threshold. The interaction constructs (Z×X1, Z×X2, and Z×X3) also demonstrate low HTMT values, with the highest value of 0.436, which is still within acceptable limits. These findings confirm that all constructs in

this study are discriminant valid, meaning that Consumer Data Security, Regulatory Compliance, and Privacy Policy Transparency measure different concepts and independently explain Purchase Decision. Additionally, Trust Level as a moderating variable is empirically distinct and appropriately interacts with the independent variables in the research model.

2. Structural Model Results (Inner Model)

The R-square values were evaluated to assess the predictive power of the structural model and the proportion of variance explained by the independent variables.

Table 4. R-Square Values

Endogenous Variable	R-square	R-square Adjusted
Purchase Decision (Y)	0.389	0.378

Source: Data Processing (2026)

The R-square value for Purchase Decision (Y) is 0.389, while the adjusted R-square value is 0.378. This indicates that Consumer Data Security, Regulatory Compliance, and Privacy Policy Transparency, along with the moderating effect of Trust Level, explain 38.9% of the variance in Purchase Decision. According to the recommended criteria, an R-square value of 0.75 is considered substantial, 0.50 moderate, and 0.25 weak. Therefore, the R-square value of 0.389 falls into the moderate category, indicating that the independent variables in this study have a moderate explanatory power in predicting purchase decisions. The remaining 61.1% of the variance is influenced by other factors not included in this research model. The f-square values were examined to evaluate the effect size of each exogenous construct on the endogenous variable in the structural model.

Table 5. f-square values

Construct	Purchase Decision (Y)
Consumer Data Security (X1)	0.060
Regulatory Compliance (X2)	0.079
Privacy Policy Transparency (X3)	0.047

Table 6. Path coefficients

Path Relationship	β (Original Sample)	Mean (M)	Std. Dev (STDEV)	T-Statistic	P-Value
Consumer Data Security on Purchase Decision	0.194	0.197	0.040	4.789	0.000
Regulatory Compliance on Purchase Decision	0.221	0.222	0.039	5.677	0.000
Privacy Policy Transparency on Purchase Decision	0.171	0.172	0.045	3.843	0.000
Trust Level on Purchase Decision	0.115	0.119	0.047	2.462	0.014
Trust Level moderating Consumer Data Security on Purchase Decision	0.222	0.221	0.043	5.143	0.000
Trust Level moderating Regulatory Compliance on Purchase Decision	0.202	0.200	0.045	4.451	0.000
Trust Level moderating Privacy Policy Transparency on Purchase Decision	0.399	0.393	0.046	8.726	0.000

Source: Data Processing (2026)

The path coefficient results indicate that all direct and moderating effects in the model are statistically significant, as all T-statistics exceed 1.96 and all p-values are below 0.05. First, Consumer Data Security has a positive and significant effect on Purchase Decision ($\beta = 0.194$, $t = 4.789$, $p = 0.000$). This indicates that stronger consumer data security increases consumers' likelihood of making purchase decisions. Therefore, the hypothesis stating that Consumer Data Security positively affects Purchase Decision is supported. Second,

Construct	Purchase Decision (Y)
Trust Level (Z)	0.021
$Z \times X3$	0.260
$Z \times X2$	0.052
$Z \times X1$	0.077

Source: Data Processing (2026)

The f-square results indicate the effect size of each construct on Purchase Decision (Y). Based on the criteria (0.02 = small, 0.15 = medium, 0.35 = large), Consumer Data Security (X1) has a small effect (0.060), Regulatory Compliance (X2) also shows a small effect (0.079), and Privacy Policy Transparency (X3) has a small effect size (0.047). Trust Level (Z) also shows a small effect on Purchase Decision with a value of 0.021. However, the interaction effect between Trust Level and Privacy Policy Transparency ($Z \times X3$) shows a medium effect size (0.260), indicating that trust strengthens the influence of privacy policy transparency on purchase decisions. Meanwhile, the moderating effects of $Z \times X1$ (0.077) and $Z \times X2$ (0.052) fall into the small effect category. These findings suggest that Trust Level plays a more substantial moderating role in strengthening the relationship between Privacy Policy Transparency and Purchase Decision compared to other relationships in the model.

The path coefficients were evaluated to test the research hypotheses and examine the relationships between the constructs in the structural model.

Regulatory Compliance also has a positive and significant effect on Purchase Decision ($\beta = 0.221$, $t = 5.677$, $p = 0.000$). This means that higher regulatory compliance enhances consumer confidence in making purchase decisions. Among the direct effects, Regulatory Compliance shows the strongest influence on Purchase Decision. Thus, the corresponding hypothesis is accepted.

Third, Privacy Policy Transparency significantly and positively affects Purchase Decision ($\beta = 0.171$, $t = 3.843$, $p =$

0.000). This suggests that when consumers clearly understand the privacy policies, they are more likely to proceed with a purchase. Hence, this hypothesis is also supported.

In addition, Trust Level has a positive and significant direct effect on Purchase Decision ($\beta = 0.115$, $t = 2.462$, $p = 0.014$). Although the coefficient is smaller than the other predictors, this result confirms that consumer trust plays an important role in influencing purchase decisions. Regarding the moderating effects, Trust Level significantly moderates the relationship between Consumer Data Security and Purchase Decision ($\beta = 0.222$, $t = 5.143$, $p = 0.000$). This indicates that when trust levels are higher, the positive impact of consumer data security on purchase decision becomes stronger.

Similarly, Trust Level significantly moderates the relationship between Regulatory Compliance and Purchase Decision ($\beta = 0.202$, $t = 4.451$, $p = 0.000$). This suggests that trust enhances the positive influence of regulatory compliance on consumers' purchase decisions.

Finally, Trust Level significantly moderates the relationship between Privacy Policy Transparency and Purchase Decision ($\beta = 0.399$, $t = 8.726$, $p = 0.000$). This is the strongest moderating effect in the model, indicating that trust substantially strengthens the impact of privacy policy transparency on purchase decisions. Overall, the findings demonstrate that Consumer Data Security, Regulatory Compliance, and Privacy Policy Transparency positively influence Purchase Decision, both directly and through the moderating role of Trust Level. Trust Level not only directly affects Purchase Decision but also strengthens the relationships between the independent variables and Purchase Decision, particularly in the relationship between Privacy Policy Transparency and Purchase Decision.

Discussion

The findings of this study indicate that consumer data security has a positive and significant impact on consumer purchase decisions in online shopping contexts. This result supports the Theory of Planned Behavior (TPB) (Ajzen, 1991), which states that positive attitudes toward a behavior in this case, perceived data security shape behavioral intentions and actual consumer actions. When consumers feel that their personal information is well protected, they demonstrate higher levels of trust toward the platform, which ultimately influences their purchase decisions. Consumer data security therefore plays a crucial role in shaping online purchasing behavior.

These findings are consistent with Zahwani et al. (2023), who emphasize that legal protection of personal data is essential for preventing cybercrime and maintaining consumer trust. In the e-commerce context, consumers' perceptions of data security are among the primary considerations in deciding whether to engage in digital transactions. This is further supported by Sihombing et al. (2024), who highlight that strong data protection systems are essential in creating a sense of safety for digital consumers. Similarly, Chaniago et al. (2025) identify that weaknesses in data security are a major reason why consumers hesitate to conduct online transactions.

Regulatory compliance also shows a significant relationship with purchase decisions. Law No. 27 of 2022 on Personal Data Protection, which has been effective since 2024, provides legal certainty regarding consumer privacy protection. As stated by indonesia.go.id (2024), the implementation of this regulation strengthens consumers' sense of security while also serving as a legal foundation that encourages businesses to manage consumer data responsibly.

From a theoretical perspective, regulatory compliance functions as a positive determinant of purchase decisions. Consumers perceive legal compliance as an indicator of professionalism and responsibility in e-commerce platforms. Within the TPB framework, enforced regulations create a subjective norm suggesting that engaging with legally compliant platforms is socially and ethically appropriate behavior. This aligns with Sri Lestari Poernomo (2023), who emphasizes the role of regulatory compliance in building consumer credibility and perceived safety.

Privacy policy transparency also demonstrates a significant influence on purchase decisions. When consumers have clear and easily accessible information regarding how their data is collected, used, and stored, they experience greater perceived behavioral control over their personal information. This increased sense of control strengthens their willingness to continue engaging in online transactions. These findings are consistent with Maharani & Prakoso (2024) and Humaira (2024), who argue that transparency in data management enhances consumer trust and loyalty. Aziz (2022) further supports this finding by stating that transparency in privacy policies directly reduces consumer concerns regarding data misuse and increases purchase intention. Consumers tend to feel more comfortable when they understand how their personal data is handled, which positively affects their willingness to engage in e-commerce transactions.

Interestingly, this study also finds that consumer trust moderates the relationship between all three independent variables and purchase decisions. This moderating effect is strongly aligned with Trust-Based Theory, which emphasizes that trust serves as a central mechanism for reducing uncertainty and perceived risk in business relationships (Morgan, 2015). Consumers with higher levels of trust are more likely to proceed with purchases even when some level of privacy risk remains. This finding is supported by Garbarino (2014), who states that trust strengthens the relationship between satisfaction and long-term loyalty in consumer-service provider relationships.

Moreover, consumer trust strengthens the relationship between data security, regulatory compliance, and privacy transparency with purchase decisions. When consumers believe that their data is secure, that platforms comply with regulations, and that privacy policies are transparent, their trust in e-commerce platforms increases significantly. This aligns with Hermansyah & Astini (2024), who argue that ethical and legally compliant digital marketing strategies enhance brand trust and increase conversion rates. Notably, the strongest moderating effect of trust is found in the

relationship between privacy policy transparency and purchase decisions, as indicated by a moderate effect size (f^2). This suggests that when consumers trust a platform, they place greater value on transparency and are more likely to engage in transactions compared to situations with lower trust levels.

Overall, the findings of this study provide both theoretical and practical implications for the development of digital commerce systems. Theoretically, this research reinforces TPB and Trust-Based Theory by demonstrating that consumer behavior in e-commerce is shaped not only by functional attributes such as security and regulation but also by psychological factors such as trust. Practically, the results highlight that businesses must prioritize data protection, regulatory compliance, and transparency not merely as technical or legal requirements, but as strategic instruments for building sustainable consumer trust.

Furthermore, in an increasingly competitive digital market, enhancing trust through ethical data management and transparent communication can significantly improve consumer loyalty and conversion rates. Therefore, trust and data protection should be positioned as core strategic assets in digital marketing, rather than secondary operational considerations.

Conclusion

This study confirms that consumer data protection is a critical factor in shaping purchasing behavior in the digital environment. Data security, regulatory compliance, and privacy policy transparency have been proven to foster consumer trust, which ultimately influences their decisions to engage in online transactions. Consumer trust not only emerges as an outcome of effective data protection practices but also acts as a reinforcing mechanism that strengthens the relationship between data protection efforts and purchase decisions. In other words, the higher the level of trust consumers have in digital service providers, the more likely they are to proceed with purchase transactions when they perceive that their personal data is well protected.

From a practical perspective, it is essential for digital business practitioners to position consumer data protection as a strategic priority by implementing robust security systems, ensuring compliance with data protection regulations, and communicating privacy policies transparently to build and sustain long-term trust. For regulators and policymakers, strengthening clear, firm, and adaptive regulations that keep pace with technological advancements is necessary, along with providing practical guidelines and enforcing effective supervision to ensure that organizations fulfill their data protection responsibilities. Furthermore, this study provides opportunities for future research to expand the scope by incorporating broader variables or different methodological approaches, such as examining psychological aspects of consumer behavior or exploring the role of data protection in other digital sectors, including fintech and edutech.

Reference

- 20.detik.com. (2025). Video BPKN soal Pengaduan Konser Korea: 500 Laporan-Total Kerugian Capai Rp 6 M. *Detikupdate*. <https://20.detik.com/detikupdate/20250207-250207056/video-bpkn-soal-pengaduan-konser-korea-500-laporan-total-kerugian-capai-rp-6-m?>
- adminteknobgt. (2023). Cara Menghitung Rumus Cochran. *Www.Teknobgt.Com*. <https://www.teknobgt.com/239258/cara-menghitung-rumus-cochran.html>
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Aziz, A. (2022). Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan Vol.9 Nomor 2 Desember 2022. *Surya Kencana* 2, 9(2), 174–182.
- BPKN-RI. (2023). RILIS-Hasil-Survey,-indeks-kualitas-layanan-penggunaan-E-commerce. *Badan Perlindungan Konsumen Republik Indonesia*, 32.
- BPKN-RI. (2024). BPKN RI Paparkan Catatan Akhir Tahun 2024, Terima 1733 Pengaduan Selama Tahun 2024. *BPKN.Go.Id*. <https://bpkn.go.id/beritaterkini/detail/bpkn-ri-paparkan-catatan-akhir-tahun-2024-terima-1733-pengaduan-selama-tahun-2024?>
- Chaniago, A. M., Siregar, M., Arifiyanto, J., & Utara, U. S. (2025). PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI KONSUMEN DALAM TRANSAKSI E-COMMERCE SHOPEE PENDAHULUAN E-Commerce merupakan bentuk perdagangan yang paling terpengaruh oleh perkembangan teknologi informasi (Putri, 2023). Perdagangan ini mengubah gagasan tradis. *Universitas Sumatera Utara*, 4307(27), 184–195.
- Dr. Ginanjar Rahmawan. (2023). 7 langkah menyusun perencanaan skripsi, tesis, disertasi dan artikel ilmiah: Vol. RMC 2.5 (G. Rahmawan (ed.); Dr. Gin White Book). Dr. Gin Research Model canvas.
- Garbarino, E. (2014). The Different Roles of Satisfaction, Trust, and Commitment in Customer Relationships. *Journal of Marketing*, April 1999. <https://doi.org/10.2307/1251946>
- Hatta Setiabudhi, S.E, M. A., Suwono, S.E, M. S., Yudi Agus Setiawan, S.S, M. ., & Syahrul Karim, M. S. (2025). Kuantitatif dengan smart pls. *Ebooks.Borneonovelty.Com*, 1–115. <https://ebooks.borneonovelty.com/media/publications/588838-analisis-data-kuantitatif-dengan-smartpls-29069ce4.pdf?>
- Hermansyah, D., & Ida Astini, B. (2024). Penerapan Strategi Pemasaran Digital dalam Meningkatkan Visibilitas dan Pertumbuhan Bisnis di Era Digital. *Seminar Nasional LPPM UMMAT*, 3, 31–48.

12. Humaira, Mayla, muhammad irwan. (2024). Kata kunci: Privasi Data, Keamanan Data, Solusi, E-Commerce. *Universitas Islam Negeri Sumatera Utara*, 3(9).
13. indonesia.go.id. (2024). Era Baru Perlindungan Data Pribadi. *Indonesia.Go.Id*. <https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi?>
14. Kredivo & Katadata. (2023). Laporan Perilaku Konsumen Indonesia 2023: Pemulihan Ekonomi dan Tren Belanja Pasca Pandemi. *Kredivocorp.Com*, 102. <https://kredivocorp.com/wp-content/uploads/2023/06/2023-Indonesia-e-Commerce-Behavior-Report.pdf>
15. Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital. *Jurnal Usm Law Review*, 7(1), 333. <https://doi.org/10.26623/julr.v7i1.8705>
16. Morgan, R. M. (2015). The Commitment-Trust Theory of Relationship Marketing. *Journal of Marketing*, December. <https://doi.org/10.2307/1252308>
17. Ph.D. Ummul Aiman, S. P. D. K. A. S. H. M. A. Ciq. M. J. M. P., Suryadin Hasda, M. P. Z. F., M.Kes. Masita, M. P. I. N. T. S. K., & M.Pd. Meilida Eka Sari, M. P. M. K. N. A. (2023). Metodologi Penelitian Kuantitatif. In *Yayasan Penerbit Muhammad Zaini*.
18. R. Gunawan Sudarmanto. (2013, April 15). *Penentuan Besarnya Sampel Menggunakan Rumus Cochran*. Masanepagmail. <https://www.scribd.com/document/135944893/Penentuan-Besarnya-Sampel-Menggunakan-Rumus-Cochran>
19. rizka zulfikar, fifian permatasari. (2024). Teori, Metode dan Praktik Penelitian Kualitatif. In evi damayanti (Ed.), *repository.penerbitwidina.com* (Vol. 7, Issue 2).
20. Selya, A. S., Rose, J. S., Dierker, L. C., Hedeker, D., Mermelstein, R. J., Saverio, D., & Costa, J. (2012). *A practical guide to calculating Cohen ' s f 2 , a measure of local effect size , from PROC MIXED*. 3(April), 1–6. <https://doi.org/10.3389/fpsyg.2012.00111>
21. Sihombing, R. E., Gede, M., Karma, S., Hukum, F., & Udayana, U. (2024). Perlindungan Konsumen dalam E-Commerce di Indonesia (Hambatan Penerapan Regulasi Antara Penerapan Dan Pengawasan). *Universitas Udayana*, 6, 58–70.
22. Sri Lestari Poernomo. (2023). Analisis Kepatuhan Regulasi Perlindungan Konsumen dalam E-Commerce di Indonesia. *Review-Unes.Com*, 6(1), 1772–1782.
23. V.Wiratna Sujarweni. (2024). *Metodologi Penelitian lengkap, praktis dan mudah dipahami* (wiratna sujarweni (ed.)). Pustakabarupress.
24. Widodo, S., Ladyani, F., Asrianto, L. O., Rusdi, Khairunnisa, Lestari, S. M. P., Wijayanti, D. R., Devriany, A., Hidayat, A., Dalfian, Nurcahyati, S., Sjahriani, T., Armi, Widya, N., & Rogayah. (2023). Metodologi Penelitian. In *Cv Science Techno Direct*.
25. Zahwani¹, S. T., Irwan, M., & Nasution², P. (2023). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital. *Analisis Kesadaran Masyarakat (Zahwani, Dkk.) JoSES: Journal of Sharia Economics Scholar*, 2(2), 105–109. <https://doi.org/10.5281/zenodo.12608751>
26. zulfa ardhini. (2023, March 8). *Skala Likert 5 poin adalah alat yang umum digunakan dalam penelitian untuk mengukur sikap, pendapat, dan persepsi responden terhadap suatu pernyataan atau pertanyaan*. <https://www.detik.com/bali/berita/d-6607480/pengertian-skala-likert-metode-dan-contohnya-untuk-penelitian?>