Published by Yayasan Amerta Insan Unggul

DOI: 10.65246

p-ISSN 3063-9840 | e-ISSN 3063-8194

GoodWill Journal of Economics, Management, and Accounting

journal homepage: https://jurnal.amertainstitute.com/index.php/GoodWill/index



Personal Data Protection Awareness Under Indonesia's PDP Law: The Role of Privacy Concern, Digital Literacy, and Institutional Trust in Privacy Protection Behavior

Laksmono Hadi[1], Fiter Abadi[2]

Master's Degree in Business Administration, Faculty of Business and Communication, Swiss German University

Email: laksmonohadi@gmail.com

ARTICLE INFO

Keywords:
Personal Data Protection Law; Privacy Protection Behavior; Perceived Concern; Digital Literacy; Institutional Trust.

Publication History:
Received: 20 May 2026
Screening: 05 May 2026
Review: 28 June 2026
Revision requested: 28 July 2026
Revised: 10 August 2026
Accepted: 31 October 2026

ABSTRACT

The implementation of Law Number 27 of 2022 concerning Personal Data Protection represents a significant milestone in strengthening privacy governance in Indonesia. However, the continued occurrence of personal data breaches suggests that legal regulation alone is insufficient to promote responsible privacy protection behavior among digital users. This study aimed to develop an integrated behavioral model to explain privacy protection behavior among Indonesian digital users by combining Protection Motivation Theory, Privacy Calculus Theory, and Institutional Theory. A quantitative research design was employed, and the data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The findings revealed that digital literacy was the strongest predictor of perceived concern, which subsequently exerted the greatest influence on privacy protection behavior. These results highlight the importance of digital literacy in shaping privacy concerns and encouraging individuals to adopt protective behaviors in digital environments. This study contributes to the integration of motivational, economic, and institutional perspectives in explaining privacy protection behavior. Practically, the findings suggest that strengthening digital literacy, institutional trust, and privacy awareness is essential to promoting responsible data protection practices and supporting the effective implementation of Indonesia's Personal Data Protection Law.

1. Introduction

The rapid expansion of digital technologies has transformed how individuals, businesses, and public institutions communicate, conduct transactions, and manage information. Artificial intelligence, cloud computing, mobile applications, big-data analytics, and digital platforms have increased connectivity and enabled information to be generated, processed, and exchanged across organizational and geographical boundaries (Organisation for Economic Co-operation and Development [OECD], 2024a, 2024b). Although digitalization improves service accessibility, operational efficiency, financial inclusion, and data-driven decision-making, growing dependence on digital systems also increases exposure to privacy violations, cyberattacks, identity theft, fraud, and unauthorized use of personal information (OECD, 2024c; Solove, 2023). Personal data has consequently become a strategic digital asset for organizations seeking to personalize services, predict consumer demand, and improve decision-making (Birch et al., 2021; OECD, 2022). Governments also rely on personal information to deliver digital identity, taxation, healthcare, social protection, and electronic public services (OECD, 2019; World Bank, 2023). However, inadequate data protection can result in financial losses, reputational damage, discrimination, and declining public trust (European Union Agency for Cybersecurity [ENISA], 2024; OECD, 2022).

Indonesia provides a relevant context for examining these challenges because of its rapid digitalization and expanding use of e-commerce, digital banking, financial technology, and electronic government services. By 2025, Indonesia had more than 221 million internet users, representing approximately 79% of its population (We Are Social & Meltwater, 2025). This expansion has strengthened

DOI: 10.65246

Indonesia's position in the ASEAN digital economy while increasing the volume of personal information circulating across digital platforms (Google et al. 2024). Nevertheless, major data-security incidents involving Tokopedia, BPJS Kesehatan, voter information, financial institutions, and government infrastructure have demonstrated persistent vulnerabilities. In 2024, a ransomware attack against the National Data Center disrupted services across more than 210 government institutions (Reuters, 2024). These incidents indicate that technological advancement and regulatory intervention alone cannot guarantee effective privacy protection.

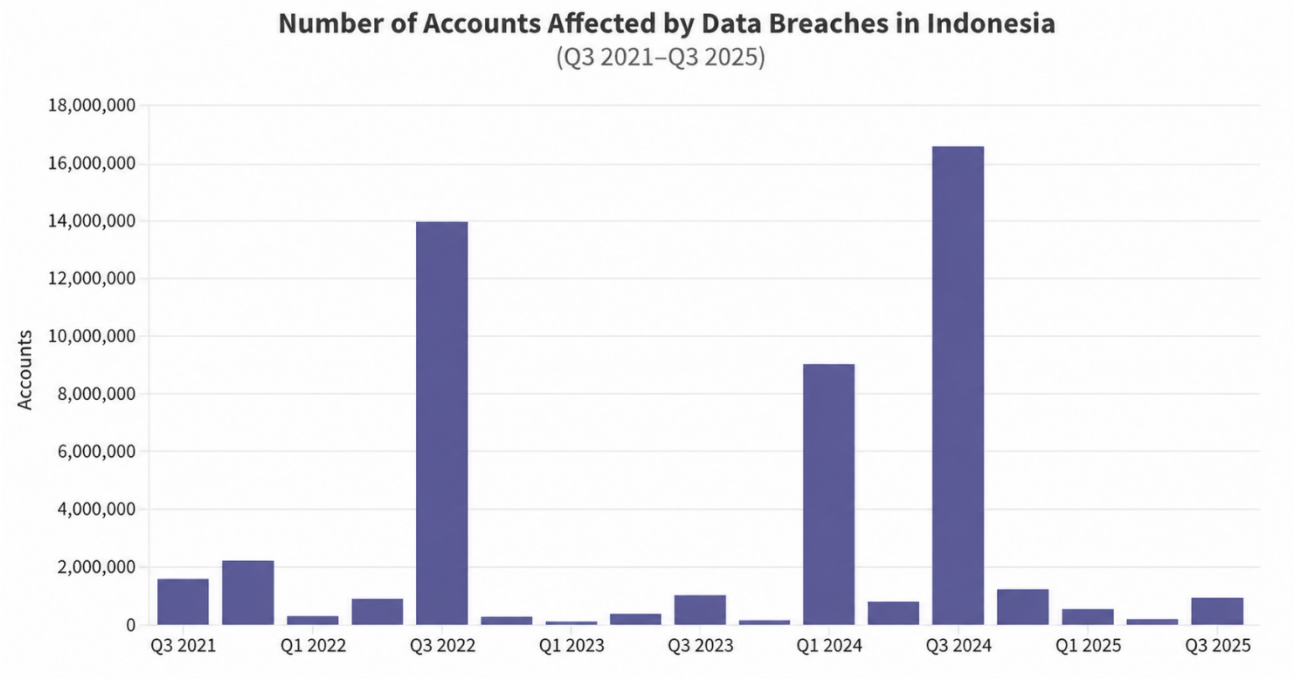


Fig. 1. Number of Breached Accounts in Indonesia, 2021–2025
Source: Surfshark (DataIndonesia.id).

In response to these challenges, Indonesia enacted Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), establishing data-subject rights and obligations for personal-data controllers and processors throughout the data-processing lifecycle (Republic of Indonesia, 2022). Although this legislation provides a comprehensive legal foundation for personal-data governance, its effectiveness also depends on individual behavior. Digital users make daily decisions about password security, privacy settings, application permissions, information disclosure, software updates, and suspicious online activities. Individuals may recognize privacy threats yet continue risky practices, including password reuse and excessive information disclosure (Acquisti et al., 2015; ENISA, 2024). Therefore, understanding personal-data protection requires examining how individuals translate privacy awareness into actual protective behavior rather than focusing exclusively on legal compliance or technological safeguards.

Previous studies have identified privacy concerns, perceived risks, institutional trust, digital literacy, prior experiences, and information-disclosure decisions as relevant determinants of privacy-related behavior (Bélanger & Crossler, 2011; Martin & Murphy, 2017; Smith et al., 2011). However, three gaps remain. First, a **theoretical gap** exists because behavioral, cognitive, and institutional determinants are often examined through separate theoretical perspectives, limiting an integrated understanding of their relationships. Second, an **empirical gap** concerns the limited contextual transferability of findings from developed economies, particularly North America and Europe, to Indonesia, where digital infrastructure, literacy, and regulatory maturity may differ (OECD, 2022). Third, a **contextual gap** involves the insufficient understanding of how individual experiences, benefit and risk perceptions, institutional trust, and digital literacy relate to actual protective behavior within Indonesia's evolving personal-data protection

DOI: 10.65246

framework. These gaps create a need for an integrated and empirically testable explanation of privacy protection behavior among Indonesian digital users.

To address these gaps, this study develops an integrated behavioral framework combining the Theory of Planned Behavior (Ajzen, 1991), Protection Motivation Theory (Rogers, 1983), Privacy Calculus Theory (Dinev & Hart, 2006), and Institutional Theory (Scott, 2014). The framework examines previous experience, benefit and risk perception, institutional trust, and digital literacy as antecedents of perceived concern, while positioning perceived concern as a predictor of personal-data protection behavior and a potential mediator of the relationships between these antecedents and protective behavior. By integrating these perspectives, the study examines how experiential, cognitive, institutional, and digital-capability factors may jointly explain individuals' privacy-related decisions.

Accordingly, this study aims to examine the determinants of personal-data protection behavior among Indonesian digital users in the context of the implementation of Law No. 27 of 2022. Specifically, it investigates whether previous experience, benefit and risk perception, institutional trust, and digital literacy influence perceived concern; whether perceived concern influences personal-data protection behavior; and whether perceived concern mediates the relationships between these antecedents and protective behavior.

This study offers three contributions. Theoretically, it integrates complementary behavioral and institutional perspectives into a unified framework for explaining personal-data protection behavior. Empirically, it extends privacy research to Indonesia, an emerging digital economy experiencing rapid technological adoption and the development of comprehensive personal-data protection regulation. Practically, it provides insights for policymakers, digital-platform providers, financial institutions, and other data-processing organizations seeking to improve privacy communication, strengthen digital literacy, and develop more effective data-protection strategies. The study's novelty lies in examining perceived concern as a potential behavioral mechanism linking individual experience, benefit and risk perceptions, institutional trust, and digital literacy with protective action. It therefore emphasizes that effective implementation of Indonesia's PDP Law depends not only on formal regulation and organizational compliance but also on individuals' capacity to recognize privacy risks and consistently adopt protective behaviors.

2. Literature Review

2.1. Conceptual and Theoretical Foundations

Personal data protection behavior refers to individuals' preventive and defensive actions to safeguard personal information against unauthorized access, misuse, exposure, and theft. These actions include using strong passwords, adjusting privacy settings, limiting information disclosure, reviewing application permissions, monitoring accounts, and adopting additional security measures. This study integrates the Theory of Planned Behavior (TPB), Protection Motivation Theory (PMT), Privacy Calculus Theory, and Institutional Theory to explain how individual experience, benefit and risk perception, institutional trust, and digital literacy relate to perceived concern and privacy protection behavior (Ajzen, 1991; Dinev & Hart, 2006; Rogers, 1983; Scott, 2014).

TPB explains how attitudes, subjective norms, and perceived behavioral control shape behavioral intentions and actions (Ajzen, 1991). PMT complements this perspective by explaining protective responses through threat appraisal and coping appraisal (Rogers, 1983). Privacy Calculus Theory explains how individuals evaluate the anticipated benefits of digital services against the potential risks of disclosing personal information (Dinev & Hart, 2006). Institutional Theory emphasizes the influence of formal regulations, organizational accountability, and institutional legitimacy on individual perceptions and behavior (Scott, 2014). Within this integrated framework, perceived concern represents the psychological mechanism through which individuals evaluate privacy threats, while digital literacy provides the capability to recognize risks and manage privacy settings. Institutional trust reflects confidence in the ability and commitment of governments, regulators, organizations, and digital platforms to protect personal information.

2.2. Review of Empirical Studies

Previous privacy research has examined the relationships between privacy concerns, risk

DOI: 10.65246

perceptions, trust, information disclosure, and protective behavior. Bélanger and Crossler (2011) reviewed information privacy research and highlighted the importance of individual and organizational factors in understanding privacy-related decisions. Smith et al. (2011) synthesized the development of information privacy research, emphasizing privacy concerns and their role in individuals' responses to information practices. Martin and Murphy (2017) examined the implications of consumer privacy research for marketing and organizational practices, underscoring the importance of understanding how personal information is collected and used. Acquisti et al. (2015) further discussed the behavioral and economic dimensions of privacy decisions, including the potential discrepancy between expressed privacy concerns and actual disclosure behavior.

These studies establish that privacy-related decisions involve more than technical security measures or formal regulation. However, their broad research orientations do not, by themselves, establish how previous experience, combined benefit and risk perception, institutional trust, and digital literacy jointly relate to perceived concern and privacy protection behavior among Indonesian digital users. The present study addresses this issue by examining these constructs within a unified behavioral framework. Its emphasis is on explaining the relationships among the proposed variables rather than treating privacy concern, institutional trust, and digital capability as isolated determinants.

2.3. Identification of the Research Gap

Three research gaps motivate this study. First, the theoretical gap concerns the limited integration of behavioral, motivational, economic, and institutional perspectives into a single framework explaining personal data protection behavior. Second, the contextual gap concerns the need to examine privacy-related behavior in Indonesia, where rapid digitalization and the implementation of Law No. 27 of 2022 concerning Personal Data Protection create a distinctive regulatory and technological context. Third, the explanatory gap concerns how previous experience, benefit and risk perception, institutional trust, and digital literacy relate to perceived concern and how perceived concern relates to protective behavior. Although existing literature provides important foundations for understanding privacy decisions, the relationships among these constructs require further examination in the Indonesian context. Accordingly, this study proposes an integrated model in which perceived concern serves as the central psychological mechanism connecting individual and institutional factors with privacy protection behavior.

2.4. Development of the Conceptual Framework

The conceptual framework positions previous experience, benefit and risk perception, institutional trust, and digital literacy as antecedents of perceived concern, while privacy protection behavior constitutes the outcome variable. Previous experience represents direct or indirect exposure to cybersecurity incidents, phishing, online fraud, data breaches, or personal information misuse. Benefit and risk perception captures individuals' evaluation of the advantages of digital services and the potential consequences of personal information disclosure. Institutional trust reflects confidence in the capability, accountability, transparency, and enforcement practices of institutions responsible for personal data protection. Digital literacy refers to individuals' ability to understand digital environments, recognize privacy threats, evaluate information disclosure, and manage digital security.

Perceived concern reflects individuals' psychological evaluation of privacy threats, including perceived vulnerability and the potential consequences of unauthorized access, data misuse, and identity theft. The framework proposes that previous experience and digital literacy strengthen threat recognition, while benefit and risk perception shapes individuals' evaluation of digital participation. Institutional trust is expected to reduce uncertainty about data management and consequently lower perceived concern. Perceived concern, in turn, is expected to encourage privacy protection behavior, including secure password practices, selective information disclosure, privacy-setting management, and account monitoring.

DOI: 10.65246

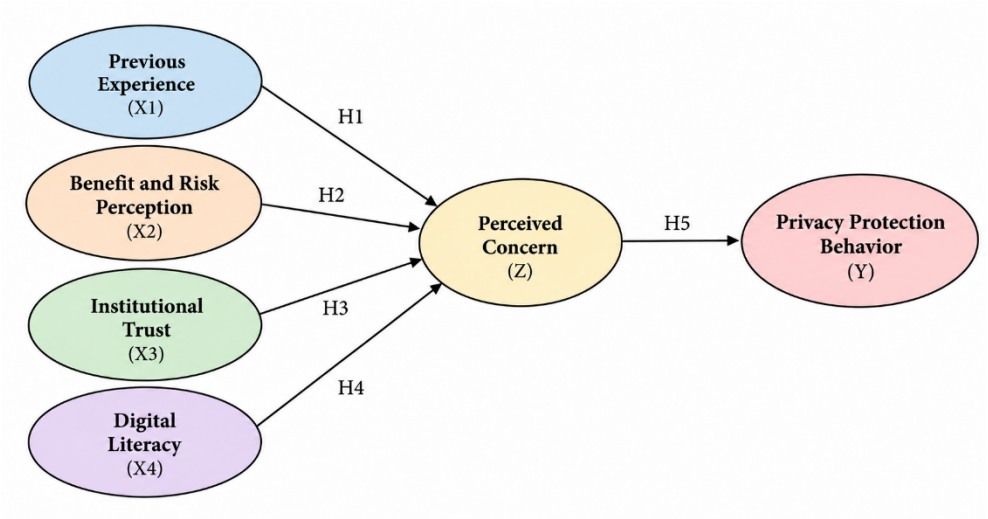


Fig. 1. Conceptual Research Framework

The framework therefore specifies five hypothesized relationships: four relationships between the antecedent variables and perceived concern, and one relationship between perceived concern and privacy protection behavior. The model provides a basis for examining how individual experience, cognitive evaluation, institutional confidence, and digital capability relate to protective actions among Indonesian digital users.

2.5. Hypotheses or Research Propositions

2.5.1. Previous Experience and Perceived Concern

Previous experience can shape individuals' understanding of privacy threats through direct or indirect exposure to cybersecurity incidents, online fraud, phishing, and personal data misuse. Such exposure may increase awareness of potential harm and encourage greater vigilance toward personal information. From a behavioral-learning perspective, previous encounters provide information that influences subsequent threat evaluation. Therefore, individuals with greater exposure to privacy-related incidents are expected to demonstrate stronger perceived concern.

H1: Previous experience positively influences perceived concern toward personal data protection.

2.5.2. Benefit and Risk Perception and Perceived Concern

Privacy Calculus Theory explains that individuals evaluate the anticipated benefits of digital services against the potential risks of personal information disclosure (Dinev & Hart, 2006). Although convenience, efficiency, accessibility, and personalization may encourage digital participation, risks involving identity theft, unauthorized access, and data misuse may intensify privacy concerns. When individuals recognize the potential consequences of personal data exposure, their perceived concern is expected to increase. Accordingly, the combined evaluation of benefits and risks is hypothesized to have a positive relationship with perceived concern, consistent with the proposed model's operationalization of this construct.

H2: Benefit and risk perception positively influences perceived concern toward personal data protection.

2.5.3. Institutional Trust and Perceived Concern

Institutional Theory emphasizes the role of formal rules, organizational accountability, and institutional legitimacy in shaping individual perceptions (Scott, 2014). Individuals often depend on governments, regulatory authorities, organizations, and digital platforms to protect information that they cannot independently monitor. Confidence in institutional capability, regulatory enforcement, transparency, and organizational accountability may reduce uncertainty regarding personal data management. Consequently, greater institutional trust is expected to reduce perceived concern about personal data protection.

H3: Institutional trust negatively influences perceived concern toward personal data protection.

2.5.4. Digital Literacy and Perceived Concern

Digital literacy enables individuals to recognize cybersecurity threats, understand data collection practices, evaluate privacy risks, and manage security settings. More digitally literate

DOI: 10.65246

individuals may be better equipped to identify vulnerabilities and understand the potential consequences of personal information exposure. Consistent with the proposed framework, digital literacy is expected to strengthen the recognition and evaluation of privacy threats, thereby increasing perceived concern.

H4: Digital literacy positively influences perceived concern toward personal data protection.

2.5.5. Perceived Concern and Privacy Protection Behavior

Perceived concern represents a psychological response to perceived privacy threats and their potential consequences. Drawing on TPB and PMT, individuals who recognize privacy threats as relevant and consequential may be more motivated to adopt protective responses (Ajzen, 1991; Rogers, 1983). Such responses include using strong passwords, managing privacy settings, limiting personal information disclosure, monitoring accounts, and avoiding suspicious online activities. Therefore, stronger perceived concern is expected to be associated with more extensive privacy protection behavior.

H5: Perceived concern positively influences privacy protection behavior.

In summary, the five hypotheses establish the proposed relationships between the four antecedent variables, perceived concern, and privacy protection behavior. Their empirical examination is intended to clarify how individual and institutional factors relate to privacy-protective practices among Indonesian digital users in the context of Law No. 27 of 2022 concerning Personal Data Protection.

3. Research Methods

3.1. Research Design

This study employed a quantitative, cross-sectional, explanatory research design to examine the relationships among previous experience, benefit and risk perception, institutional trust, digital literacy, perceived concern, and privacy protection behavior among digital users in Indonesia. A deductive approach was adopted to formulate and empirically test hypotheses derived from the theoretical framework. Partial Least Squares Structural Equation Modeling (PLS-SEM) was conducted using SmartPLS 4 because the research model involves multiple latent constructs and examines relationships among exogenous and endogenous variables. PLS-SEM is suitable for predictive-oriented behavioral research and enables the simultaneous assessment of measurement quality and structural relationships (Hair et al., 2022).

3.2. Research Context and Setting

The study was conducted in Indonesia, where digital platforms are increasingly used for social communication, e-commerce, digital banking, online payments, and electronic public services. The enactment of Law No. 27 of 2022 concerning Personal Data Protection provides an important regulatory context for examining individual privacy protection behavior. The study focused on individuals who actively use digital services that collect or process personal information. Data were collected online to facilitate participation across different geographical areas of Indonesia.

3.3. Population and Sample / Research Participants

The target population comprised Indonesian citizens aged 17 years and above who actively used digital platforms involving the collection or processing of personal information. The unit of analysis was the individual digital user. A non-probability sampling approach combining convenience sampling and snowball dissemination was employed because a comprehensive sampling frame of Indonesian digital users was unavailable. Convenience sampling facilitated recruitment through accessible online communication channels, while snowball dissemination allowed initial participants to share the questionnaire with other potentially eligible respondents.

Participants were required to be Indonesian citizens or permanent residents living in Indonesia, be at least 17 years old, regularly use digital platforms that process personal data, and have experience with digital activities such as online transactions, communication, or public services. Only complete and eligible responses were retained. Following screening and data cleaning, **300 valid responses** were included in the analysis. This sample exceeded the preliminary minimum of 40 observations indicated by the conventional ten-times guideline, based on the maximum of four structural paths directed toward an endogenous construct. Nevertheless, sample adequacy was also considered

DOI: 10.65246

in relation to statistical power and estimation stability, consistent with contemporary PLS-SEM guidance (Hair et al., 2022).

3.4. Data Sources and Data Collection

Primary data were collected through a structured online questionnaire administered using Google Forms. Online data collection was appropriate for the target population because respondents were active digital-service users and could access the questionnaire through electronic communication channels. The questionnaire contained two sections: demographic and digital-service-use information, including age, gender, educational attainment, occupation, monthly income, and digital-service utilization; and measurement items for the research constructs. Before participating, respondents received information about the research objectives, voluntary participation, confidentiality, and anonymity. Electronic informed consent was obtained before questionnaire completion.

3.5. Measurement of Variables and Research Instruments

The research instrument measured six constructs: previous experience, benefit and risk perception, institutional trust, digital literacy, perceived concern, and privacy protection behavior. The measurement items were adapted from established studies, as indicated in the original research design. All items were assessed using a five-point Likert scale ranging from 1 (*strongly disagree*) to 5 (*strongly agree*).

Previous experience represented respondents' direct or indirect exposure to cybersecurity incidents, phishing, online fraud, data breaches, or personal data misuse. Benefit and risk perception captured respondents' evaluations of the advantages of digital services and the potential consequences of disclosing personal information. Institutional trust measured confidence in the institutions responsible for collecting, processing, and protecting personal data. Digital literacy reflected respondents' ability to understand digital environments, recognize privacy threats, and manage associated risks. Perceived concern captured respondents' concerns about unauthorized access, data misuse, exposure, and potential privacy-related harm. Privacy protection behavior represented preventive and defensive actions, including managing passwords and privacy settings, limiting information disclosure, reviewing application permissions, monitoring accounts, and adopting additional security measures.

3.6. Data Analysis Techniques

The data were analyzed using PLS-SEM in SmartPLS 4. The analysis proceeded in two main stages. First, the measurement model was evaluated to establish indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. Second, the structural model was assessed to examine collinearity, the magnitude and direction of path coefficients, explanatory power, effect sizes, and predictive relevance.

Structural relationships were evaluated using path coefficients (β), the coefficient of determination (R^2), effect sizes (f^2), and predictive relevance (Q^2). Bootstrapping with **5,000 resamples** was performed to estimate standard errors, t-statistics, p-values, and confidence intervals for hypothesis testing. Statistical significance and the direction of the estimated coefficients were used to assess the proposed relationships.

3.7. Validity, Reliability, and Trustworthiness

The quality of the measurement model was assessed using established PLS-SEM criteria (Hair et al., 2022). Indicator reliability was evaluated through outer loadings, with values of approximately 0.708 or higher considered desirable. Internal consistency reliability was assessed using Cronbach's alpha and composite reliability (CR), with values between 0.70 and 0.95 generally considered acceptable. Convergent validity was assessed using the average variance extracted (AVE), with values of at least 0.50 indicating adequate convergence. Discriminant validity was examined using the heterotrait–monotrait ratio (HTMT), with values below 0.90 indicating satisfactory distinction between constructs.

Collinearity was assessed using the variance inflation factor (VIF) before interpreting the structural relationships. The use of bootstrapping with 5,000 resamples supported the estimation of uncertainty around the structural coefficients. Together, these procedures provided a systematic basis for evaluating the reliability and validity of the measurement instruments and the robustness of the hypothesized relationships.

DOI: 10.65246

3.8. Ethical Considerations

Participation was voluntary, and respondents received information about the research objectives, confidentiality, and anonymity before completing the questionnaire. Electronic informed consent was obtained before participation. No personally identifiable information was intentionally collected, and the responses were used exclusively for academic research. Incomplete or ineligible submissions were excluded from the analysis. These procedures were intended to protect respondents' privacy and support responsible handling of research data.

3.9. Research Procedure

The research process consisted of five stages. First, the conceptual framework and hypotheses were established based on the relevant theoretical perspectives. Second, a structured questionnaire was developed using measurement items adapted from established studies. Third, the questionnaire was distributed online through Google Forms using convenience sampling and snowball dissemination. Fourth, the collected responses were screened for eligibility, completeness, duplicate submissions, and inconsistent response patterns. Finally, the 300 valid responses were analyzed using SmartPLS 4 through measurement model assessment, structural model evaluation, and bootstrapping-based hypothesis testing.

3.10. Methodological Limitations

Several methodological limitations should be acknowledged. First, the cross-sectional design captures respondents' perceptions and behaviors at a single point in time and therefore limits the ability to establish temporal or causal relationships. Second, convenience sampling and snowball dissemination constitute non-probability sampling methods, which limit the generalizability of the findings to all Indonesian digital users. Third, the online questionnaire relies on self-reported responses, which may be affected by recall errors, social desirability, or differences in respondents' interpretations of the measurement items. Accordingly, the findings should be interpreted within the context of the research design, sampling approach, and measurement procedures.

4. Results and Discussion

4.1. Research Results

4.1.1. Sample Description and Descriptive Statistics

The analysis was based on 300 valid responses from Indonesian digital users. The sample consisted of 174 males (58.0%) and 126 females (42.0%). Respondents aged above 45 years constituted the largest age group (35.7%), followed by those aged 17–24 years (28.0%). Most respondents held a bachelor's degree (50.7%), and private-sector employees represented the largest occupational group (49.3%). Regarding digital engagement, 45.0% spent more than seven hours online daily, indicating substantial exposure to digital services and personal-data processing activities.

Table 1. Respondent Characteristics

Characteristic	Category	Frequency	Percentage (%)
Gender	Male	174	58.0
	Female	126	42.0
Age	17–24 years	84	28.0
	25–34 years	51	17.0
	35–44 years	58	19.3
	Above 45 years	107	35.7
Education	High school	64	21.3
	Diploma	12	4.0
	Bachelor's degree	152	50.7
	Master's degree	72	24.0
Occupation	Private-sector employee	148	49.3
	Student	77	25.7
	Other occupations	38	12.6
	Freelancer	15	5.0
	Entrepreneur	14	4.7
	Government employee	8	2.7
Daily internet use	Less than 2 hours	3	1.0

DOI: 10.65246

2–4 hours	56	18.7
5–7 hours	106	35.3
More than 7 hours	135	45.0

Source: Researcher data (2026).

Descriptive statistics showed relatively high mean scores for five constructs, while Institutional Trust recorded a comparatively moderate score. Experience had the highest mean (M = 4.1480, SD = 0.62818), followed by Perceived Concern (M = 4.1228, SD = 0.70347), Privacy Protection Behavior (M = 4.0891, SD = 0.68013), Benefit and Risk (M = 4.0695, SD = 0.65692), and Digital Literacy (M = 3.9467, SD = 0.68644). Institutional Trust recorded the lowest mean (M = 3.0942, SD = 1.04676).

Table 2. Descriptive Statistics of Research Constructs

Construct	N	Mean	Standard deviation
Experience	300	4.1480	0.62818
Benefit and Risk	300	4.0695	0.65692
Institutional Trust	300	3.0942	1.04676
Digital Literacy	300	3.9467	0.68644
Perceived Concern	300	4.1228	0.70347
Privacy Protection Behavior	300	4.0891	0.68013

Source: Researcher data (2026).

4.1.2. Data Quality and Preliminary Analysis

The initial dataset was screened for incomplete responses, duplicate submissions, inconsistent response patterns, and multivariate outliers. Eight observations were removed during screening, leaving 300 valid responses for the final analysis. The P–P plot and histogram indicated approximately acceptable residual distribution patterns. Multicollinearity diagnostics showed tolerance values above 0.10 and VIF values ranging from 1.003 to 1.550 in the preliminary analysis, indicating no substantial multicollinearity concerns.

4.1.3. Main Analytical Results

The measurement model was evaluated using outer loadings, average variance extracted (AVE), Cronbach's alpha, composite reliability (CR), and discriminant validity assessments. All indicator loadings exceeded 0.70, ranging from 0.708 to 0.939. AVE values ranged from 0.609 to 0.689, exceeding the recommended minimum of 0.50. Cronbach's alpha values ranged from 0.851 to 0.944, while composite reliability values ranged from 0.893 to 0.943. Fornell and Larcker (1981) criterion and cross-loading assessment also supported discriminant validity.

Table 3. Measurement Model Assessment

Construct	Outer loading range	AVE	Cronbach's alpha	Composite reliability
Experience	0.708–0.840	0.625	0.851	0.893
Benefit and Risk	0.738–0.829	0.620	0.898	0.919
Institutional Trust	0.726–0.939	0.689	0.944	0.939
Digital Literacy	0.731–0.824	0.609	0.908	0.925
Perceived Concern	0.773–0.859	0.683	0.922	0.938
Privacy Protection Behavior	0.756–0.827	0.646	0.932	0.943

Source: Researcher data (2026). Assessment criteria follow Hair et al. (2022).

The structural model showed inner VIF values ranging from 1.000 to 1.591, indicating no problematic collinearity. The coefficient of determination (R^2) was 0.663 for Perceived Concern and 0.597 for Privacy Protection Behavior. The corresponding adjusted R^2 values were 0.658 and 0.596, respectively. Predictive relevance values (Q^2predict) were 0.644 for Perceived Concern and 0.467 for Privacy Protection Behavior. Both values exceeded zero.

DOI: 10.65246

Effect-size analysis indicated that Digital Literacy had the largest contribution to Perceived Concern ($f^2 = 0.569$), followed by Benefit and Risk ($f^2 = 0.173$), Experience ($f^2 = 0.058$), and Institutional Trust ($f^2 = 0.042$). Perceived Concern had a substantial effect size in explaining Privacy Protection Behavior ($f^2 = 1.482$).

Table 4. Structural Model Assessment

Endogenous construct / predictor	R^2	Adjusted R^2	f^2	Q^2predict
Perceived Concern	0.663	0.658	—	0.644
Experience → Perceived Concern	—	—	0.058	—
Benefit and Risk → Perceived Concern	—	—	0.173	—
Institutional Trust → Perceived Concern	—	—	0.042	—
Digital Literacy → Perceived Concern	—	—	0.569	—
Privacy Protection Behavior	0.597	0.596	—	0.467
Perceived Concern → Privacy Protection Behavior	—	—	1.482	—

Source: Researcher data (2026).

The model fit assessment produced an SRMR of 0.067 for the saturated model and 0.075 for the estimated model. The NFI values were 0.793 and 0.790, respectively. These values provide supplementary information on model fit, while the explanatory and predictive metrics provide additional evidence of the model's performance.

4.1.4. Hypothesis Testing Results / Key Findings

Hypothesis testing was conducted using bootstrapping with 5,000 resamples. Statistical significance was assessed using a t-statistic threshold of 1.96 and a p-value below 0.05, consistent with the procedures reported in the original study (Hair et al., 2022). The results are presented in Table 5.

Table 5. Hypothesis Testing Results

Hypothesis	Structural relationship	β (original sample)	t-statistic	p-value	Result
H1	Experience → Perceived Concern	0.169	3.806	< 0.001	Supported
H2	Benefit and Risk → Perceived Concern	0.305	5.786	< 0.001	Supported
H3	Institutional Trust → Perceived Concern	**0.120***	2.484	0.013	Direction requires verification
H4	Digital Literacy → Perceived Concern	0.499	8.378	< 0.001	Supported
H5	Perceived Concern → Privacy Protection Behavior	0.773	25.418	< 0.001	Supported

Source: Researcher data (2026).

Note: The original hypothesis-testing table reports a positive coefficient of 0.120 for H3, whereas the accompanying narrative reports a negative coefficient of −0.120. The original SmartPLS output must be checked before the final direction and decision for H3 are confirmed.

The results indicate statistically significant relationships for all five hypothesized paths. H1, H2, H4, and H5 have positive coefficients in the reported results. The sign of H3 remains inconsistent between the table and narrative and therefore requires verification before its directional hypothesis can be conclusively evaluated.

4.2. Research Discussion

4.2.1. Interpretation of Key Findings

The findings indicate that Digital Literacy is the strongest antecedent of Perceived Concern, with a path coefficient of $\beta = 0.499$ and an effect size of $f^2 = 0.569$. This suggests that the ability to understand digital environments and recognize privacy vulnerabilities plays a central role in shaping users' concerns about personal data protection. Benefit and Risk also has a positive and significant relationship with Perceived Concern ($\beta = 0.305$), indicating that individuals' evaluation of the

DOI: 10.65246

advantages and potential risks of digital services is relevant to their privacy-related perceptions. Experience has a smaller but significant positive relationship (β = 0.169), suggesting that prior exposure to digital activities and privacy-related incidents contributes to concern.

Institutional Trust requires careful interpretation because its reported path coefficient has conflicting signs in the original results. The narrative describes a negative relationship (β = −0.120), consistent with the hypothesis that greater institutional trust reduces privacy concern, whereas the hypothesis-testing table reports a positive coefficient (β = 0.120). This discrepancy must be resolved using the original SmartPLS output.

Perceived Concern has the strongest direct relationship in the model, positively influencing Privacy Protection Behavior (β = 0.773, f^2 = 1.482). Its substantial effect indicates that concern about privacy risks is closely associated with users' adoption of protective practices. The model explains 66.3% of the variance in Perceived Concern and 59.7% of the variance in Privacy Protection Behavior.

4.2.2. Comparison with Previous Studies

The findings are consistent with the theoretical explanations presented in the study. The relationship between Experience and Perceived Concern accords with Protection Motivation Theory, which emphasizes the role of threat appraisal in motivating protective responses. The positive association between Benefit and Risk and Perceived Concern is consistent with Privacy Calculus Theory, which explains how individuals evaluate the benefits and potential risks associated with disclosing personal information. The strong relationship between Digital Literacy and Perceived Concern reinforces the importance of digital competence in identifying and evaluating privacy threats.

The relationship between Perceived Concern and Privacy Protection Behavior is also consistent with the protection-motivation perspective: individuals who perceive privacy threats as personally relevant are more likely to take preventive action. However, the present results should not be treated as a definitive confirmation of all theoretical mechanisms, and direct comparisons with specific empirical studies require additional recent, relevant journal references. The Institutional Trust finding cannot be compared conclusively until the coefficient-sign discrepancy has been resolved.

4.2.3. Theoretical Contributions

This study contributes to the understanding of privacy protection behavior by bringing individual experience, benefit and risk evaluation, institutional confidence, and digital literacy into a single explanatory framework. The results identify Digital Literacy as the strongest antecedent of Perceived Concern and establish Perceived Concern as the strongest predictor of Privacy Protection Behavior within the estimated model. These findings emphasize the importance of distinguishing the factors that shape privacy concerns from the psychological response most closely associated with protective action. The study therefore extends the application of behavioral and institutional perspectives to personal data protection among Indonesian digital users.

4.2.4. Practical and Policy Implications

The findings suggest that policymakers, digital-platform providers, financial institutions, and other organizations processing personal information should prioritize practical digital-literacy initiatives. Educational programs can help users recognize phishing, understand application permissions, evaluate privacy policies, and manage account security. The strong relationship between Perceived Concern and Privacy Protection Behavior also indicates the value of clear, accessible communication about privacy risks and available protective measures.

The descriptive results further show that Institutional Trust has the lowest mean score (M = 3.0942) and the highest standard deviation (SD = 1.04676) among the constructs. This pattern suggests variation in respondents' confidence in institutional data protection. Greater transparency, visible accountability, clear communication about data breaches, and credible enforcement of personal-data protection requirements may help strengthen public confidence. However, the direction of the relationship between Institutional Trust and Perceived Concern should not inform specific directional policy claims until H3 has been verified.

4.2.5. Integration with the Research Gap

The study addresses the identified research gap by testing an integrated model of privacy

DOI: 10.65246

protection behavior in Indonesia, a context experiencing rapid digital adoption and the implementation of Law No. 27 of 2022 concerning Personal Data Protection. Rather than examining digital literacy, experience, risk evaluation, or institutional trust in isolation, the model considers their relationships with Perceived Concern and the subsequent association between concern and protective behavior. The findings show that these antecedents collectively explain a substantial proportion of variance in Perceived Concern, while Perceived Concern accounts for a substantial proportion of variance in Privacy Protection Behavior. This provides empirical evidence for an integrated behavioral explanation within the Indonesian context.

4.2.6. Acknowledgement of Study Limitations

The findings should be interpreted in light of the study's cross-sectional design, non-probability sampling, and reliance on self-reported online questionnaire responses. These features limit causal inference and generalizability to the wider population of Indonesian digital users. In addition, the reported Institutional Trust coefficient contains an unresolved sign discrepancy that must be checked against the original SmartPLS output. Future studies could use probability-based sampling, longitudinal data, and additional contextual variables to examine whether these relationships remain stable across demographic groups, digital-service categories, and changes in personal-data protection governance.

5. Conclusion

5.1. Summary of Key Findings

This study examined the determinants of privacy protection behavior among Indonesian digital users in the context of Law No. 27 of 2022 concerning Personal Data Protection. Based on data from 300 respondents analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM), the findings indicate that Experience ($\beta = 0.169$, $p < 0.001$), Benefit and Risk ($\beta = 0.305$, $p < 0.001$), and Digital Literacy ($\beta = 0.499$, $p < 0.001$) positively and significantly influence Perceived Concern. Institutional Trust also has a statistically significant relationship with Perceived Concern ($p = 0.013$), although the direction of its coefficient requires confirmation against the original SmartPLS output. Perceived Concern exhibits the strongest relationship in the model, positively influencing Privacy Protection Behavior ($\beta = 0.773$, $p < 0.001$). Overall, the findings demonstrate the importance of individual experience, risk-benefit evaluation, digital literacy, and privacy concern in understanding protective behavior among Indonesian digital users.

5.2. Theoretical Contributions

This study contributes to the literature by integrating Protection Motivation Theory, Privacy Calculus Theory, and Institutional Theory into a framework for examining privacy protection behavior. The findings identify Digital Literacy as the strongest antecedent of Perceived Concern and establish Perceived Concern as the strongest predictor of Privacy Protection Behavior within the proposed model. These results emphasize the importance of considering individual capabilities, cognitive evaluations, and institutional factors when explaining privacy-related behavior. The study also extends the application of these theoretical perspectives to Indonesia, where digital adoption and the implementation of comprehensive personal-data protection regulation create an important context for understanding individual responses to privacy risks.

5.3. Practical and Policy Implications

The findings highlight the need for sustained digital-literacy initiatives that help users recognize privacy threats, understand personal-data processing, evaluate application permissions, and implement appropriate security practices. Government agencies, educational institutions, financial institutions, and digital-service providers should strengthen privacy education and communicate data-protection risks in accessible language. Organizations should also improve transparency, accountability, and the accessibility of privacy controls to support responsible data management and public confidence. Given the strong relationship between Perceived Concern and Privacy Protection Behavior, awareness initiatives should connect risk recognition with practical actions, including stronger authentication, selective information disclosure, privacy-setting management, and avoidance of suspicious applications.

5.4. Limitations of the Study

Several limitations should be considered when interpreting the findings. First, the cross-sectional

DOI: 10.65246

design captures respondents' perceptions and reported behavior at a single point in time, limiting conclusions about behavioral changes following the continued implementation of the Personal Data Protection Law. Second, the reliance on self-reported questionnaire data may introduce social-desirability bias and differences between reported and actual protective behavior. Third, the use of voluntary online participation and non-probability sampling limits the generalizability of the findings to Indonesia's wider digital-user population. Finally, the model focuses on Experience, Benefit and Risk, Institutional Trust, and Digital Literacy as antecedents of Perceived Concern. Other potentially relevant factors, including privacy awareness, perceived vulnerability, self-efficacy, cybersecurity knowledge, technology readiness, and organizational privacy practices, were not examined.

5.5. Directions for Future Research

Future research could employ longitudinal designs to examine how privacy concerns and protective behaviors change as Indonesia's personal-data protection framework develops. Probability-based sampling and broader respondent coverage could improve the representativeness and generalizability of findings. Researchers could also compare users across age groups, educational backgrounds, and digital-service categories to identify differences in privacy-related behavior. Furthermore, incorporating variables such as privacy awareness, perceived vulnerability, self-efficacy, cybersecurity knowledge, and organizational privacy practices may provide a more comprehensive explanation of protective behavior. Finally, future studies could combine self-reported measures with observed security practices to assess whether privacy concern consistently translates into actual protective action.

6. References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

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

Bélanger, 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

Birch, K., Cochrane, D., & Ward, C. (2021). Data as asset? The measurement, governance, and valuation of digital personal data. *Big Data & Society, 8*(1). https://doi.org/10.1177/2053951721994118

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Google, Temasek, & Bain & Company. (2024). *e-Conomy SEA 2024*.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage Publications.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4

Organisation for Economic Co-operation and Development. (2019). *The path to becoming a data-driven public sector*. OECD Publishing.

Organisation for Economic Co-operation and Development. (2022). *OECD digital economy outlook 2022*. OECD Publishing.

Organisation for Economic Co-operation and Development. (2024a). *OECD digital economy outlook 2024 (Volume 1)*. OECD Publishing.

Organisation for Economic Co-operation and Development. (2024b). *OECD digital economy outlook 2024 (Volume 2)*. OECD Publishing.

Organisation for Economic Co-operation and Development. (2024c). Going Digital Toolkit. OECD Publishing.

Republic of Indonesia. (2022). *Law Number 27 of 2022 concerning Personal Data Protection*.

Reuters. (2024). *Indonesia's National Data Center ransomware attack disrupts more than 200 government agencies*.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology* (pp. 153–176). Guilford Press.

Scott, W. R. (2014). *Institutions and organizations: Ideas,*

DOI: 10.65246

interests, and identities (4th ed.). Sage Publications.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015.

Solove, D. J. (2023). *Nothing to hide: The false tradeoff between privacy and security* (Updated ed.). Yale University Press.

We Are Social, & Meltwater. (2025). *Digital 2025: Indonesia.*

World Bank. (2023). *Indonesia economic prospects.*