Tec Empresarial
P-ISSN: 1659-2395; E-ISSN: 1659-3359

Data Ethics and Privacy in the Digital Business Ecosystem

Desti Amalia Putri[A], Winnie[B], Nilla Astiti[C]

Abstract

The rapid expansion of the digital economy has transformed business operations into highly interconnected, data-driven ecosystems. While digital technologies enable efficiency, personalization, and market growth, they also raise significant concerns regarding data privacy, security, and ethical responsibility. Repeated data breach incidents and weak enforcement of data protection regulations, particularly in emerging digital markets, have contributed to declining consumer trust in digital platforms. This study examines the role of digital transparency, data security, and corporate digital social responsibility (CDSR) in shaping consumer trust within the digital business context. Using a quantitative approach, data were collected from 253 active digital platform users in Indonesia through an online questionnaire and analyzed using Partial Least Squares–Structural Equation Modeling (PLS-SEM). The findings indicate that digital transparency and data security have a strong and significant influence on consumer trust, while CDSR plays an important complementary role by signaling ethical commitment beyond regulatory compliance. Based on our findings, legal compliance alone is insufficient to sustain trust without transparent communication and responsible digital practices. This research contributes to the growing literature on digital ethics by highlighting the importance of integrating transparency, security, and social responsibility into digital governance strategies. Practically, the findings offer insights for digital businesses to strengthen consumer trust by adopting ethical data management practices that go beyond minimum regulatory requirements.

Keywords: *Data Ethics, Data Privacy, Digital Business Ecosystem.*

INTRODUCTION

The digital economy has fundamentally reshaped contemporary business through highly interconnected, data-driven ecosystems. Advances in information technology have enabled organizations to enhance operational efficiency and market expansion; however, they have also intensified challenges related to data privacy, information security, and corporate ethical responsibility (Bahadur & Ali, 2023). The vast amount of data generated daily on digital platforms has made transparent and responsible data governance a critical issue for businesses, regulators, and consumers alike (Balboni & Francis, 2025).

Transparency has emerged as a central mechanism in the governance of digital platforms, closely linked to accountability and

[A]*Bina Nusantara University, Tangerang, Indonesia. Email: desti.putri@binus.ac.id*
[B]*Bina Nusantara University, Tangerang, Indonesia*
[C]*Bina Nusantara University, Tangerang, Indonesia*

consumer trust. Strzelecki & Rizun (2022) Prior empirical research suggests that increased transparency in platform operations such as data processing practices, information disclosure, and algorithmic outcomes positively influences consumer decision-making and trust formation. Fazli, 2025 As a form of soft governance, transparency can encourage responsible behavior among platform actors while complementing formal regulatory controls.

Data privacy concerns have been further amplified by the widespread adoption of big data analytics, artificial intelligence, and machine learning. Although these technologies support personalization and innovation, they also introduce ethical risks, including bias, discrimination, loss of data control, and unauthorized inference of sensitive information (Karale, 2021). Consequently, organizations face growing pressure to move beyond minimum legal compliance and adopt ethical data management practices.

Recent large-scale data breaches in Indonesia demonstrate persistent governance failures despite the implementation of personal data protection regulations, highlighting the gap between legal frameworks and effective enforcement (Doshi & Schmidt, 2024). Similarly, global regulatory regimes such as the General Data Protection Regulation (GDPR) provide important benchmarks but do not alone ensure ethically sound data practices.

In response to these challenges, Corporate Digital Social Responsibility (CDSR) has been proposed as a bridging framework between regulatory compliance and ethical data governance (Lim et al., 2025). This study therefore aims to examine the effects of Data Transparency, Regulatory Compliance, and Corporate Digital Social Responsibility on Customer Trust in the digital business context, contributing to the literature on trust formation in the digital economy.

LITERATURE REVIEW

Previous Study

The 2020 study “Digital Transparency: Dimensions, Antecedents, and Consequences for Customer Relationship Quality” by Portes, N’Goala, and Cases offers one of the most detailed empirical studies of digital transparency and its consequences for customer-brand relationships. Their research arose from growing public demand for transparency and concerns about how companies manage customer data in a rapidly digitizing market. Prior to their research, transparency was often discussed conceptually but lacked clear, multidimensional measurement. Using a survey of 445 Amazon users, analyzed through structural equation modeling, the researchers identified three core dimensions of perceived digital transparency: objectivity, clarity, and openness. These dimensions represent customers' subjective evaluations of how a brand communicates and handles digital information practices such as algorithms, data collection, recommendation engines, and targeted advertising.

The study “Scale Development and Validation of Corporate Digital Responsibility from a Consumer Perspective” by Yang and colleagues (2025) presents an important investigation into Corporate Digital Responsibility (CDR), which addresses a critical gap in the digital ethics literature, namely, the absence of a validated scale that captures CDR from a consumer perspective. Prior to this research, CDR was largely discussed conceptually or embedded within the CSR framework, with little effort to understand how consumers perceive digital responsibility as a multidimensional corporate obligation.

Data Transparency

Data transparency refers to the clarity, openness, and accessibility of information related to how organizations collect, process, and use consumer data (Gupta et al., 2025). Transparency is widely recognized as a crucial driver of user trust in digital environments. Geng (2024) argues that transparency serves a specific purpose: enabling accountability and mitigating social risks caused by algorithmic decision-making on digital platforms (Wu et al., 2024). Transparency mechanisms such as disclosure of data sources, algorithmic logic, and decision criteria help consumers evaluate whether a platform is acting fairly and responsibly.

Regulatory Compliance

Regulatory compliance refers to an organization's adherence to laws, standards, and guidelines governing data protection, privacy, and cybersecurity (Khalaf et al., 2025). Globally, the European Union's General Data Protection Regulation (GDPR) has become a benchmark for data governance, influencing regulatory frameworks worldwide (Fu et al., 2022).

In Indonesia, a series of large-scale personal data breaches from 2023 to 2025 affecting the tax system, SIM card databases, and public sector digital services demonstrates the continuing gap between regulation and practice, even after the enactment of the Personal Data Protection Law (PDP Law) (Cheng & Zhang, 2023). These incidents highlight the need for organizations to not only comply with regulations but also to implement robust governance mechanisms to prevent abuse and maintain public trust.

Digital Business

Customer trust represents the belief that a digital organization will act responsibly, securely, and ethically in handling consumer data (Doshi & Schmidt, 2024). In digital platforms where interactions are largely intangible, trust is a key determinant of user engagement, loyalty, and continued usage.

Trust is shaped by three key antecedents (Urban & Plattfaut, 2025):

1. Transparency, which reduces uncertainty about how data is used
2. Regulatory compliance, which signals organizational legitimacy

3. C-DSR, which demonstrates ethical commitment beyond legal requirements.

Research shows that when users perceive organizations to be transparent, compliant, and socially responsible, their willingness to engage with digital services increases significantly (Veltri et al., 2023; Aldboush & Ferdous, 2023). Conversely, repeated data-breach incidents, misinformation, and opaque AI practices erode public trust, regardless of legal safeguards (Zadeh et al., 2023; van der Merwe & al Achkar, 2022). In sum, customer trust acts as both the outcome and the foundation of sustainable digital business ecosystems. Strengthening trust requires holistic strategies combining transparency, compliance, and ethical digital stewardship.

METHOD

This research was conducted within the context of Indonesia's digital business ecosystem, focusing on digital service users interacting with personal data management platforms. The Indonesian context is particularly relevant given the rapid development of digital technology and the strengthening of personal data protection regulations since the enactment of the Personal Data Protection Law (PDP Law). Indonesia's heterogeneous digital environment, comprising various types of applications ranging from e-commerce and online transportation to digital banking and app-based healthcare, makes it a rich and relevant research area for understanding the dynamics of user perceptions of transparency and data management (Wirtz et al., 2023; Martínez & Martín, 2021).

The sampling technique used in this study was purposive sampling, which selects respondents based on specific criteria directly relevant to the research objectives. This technique was used based on the research needed to obtain data from respondents who have sufficient understanding and experience regarding privacy policies, data consent forms, and the use of personal information by digital companies. According to Etikan (2019), purposive sampling is particularly suitable for research requiring higher data quality than simply large quantities, as it allows researchers to select individuals who are truly knowledgeable about the issues being studied. Furthermore, this technique ensures that respondents are not selected randomly, but based on their context, experience, and involvement in digital activities related to personal data. The sample size was determined based on Structural Equation Modeling Partial Least Squares (SEM-PLS) guidelines, which recommend a minimum sample size of five to ten times the number of indicators used in the research model (Hair et al., 2021). Given that this study used between 20 and 30 indicators, the ideal sample size is in the range of 100 to 200 respondents.

This research collected data by conducting through the distribution of an online questionnaire designed using a five-point Likert scale to measure respondents' perceptions of each research variable (Reid et al., 2024). The survey instrument was carefully designed to

ensure that each question was clear, relevant, and able to capture respondents' in-depth perceptions of data management ethics (Reid & Ringel, 2025; Wu et al., 2024). The instrument also included statements related to users' experiences in reading privacy policies, understanding how their data is used, and their perceptions of the compliance and integrity of digital companies (Strzelecki & Rizun, 2022). In addition, several questions were designed to measure respondents' level of trust in digital companies regarding data security, transparency in data management, and the company's commitment to protecting their privacy rights.

RESULT AND DISCUSSION

Study Object

This study aims to make business and consumers aware of digital ethics and privacy in the digital business. Digital businesses were chosen as the focus of the study because of their significant reliance on the collection, processing, storage, and utilization of customers' personal data through applications, websites, or artificial intelligence-based systems (Urban & Plattfaut, 2025). Therefore, data transparency, regulatory compliance, and corporate digital social responsibility (C-DSR) are identified as important factors in building and maintaining customer trust.

This research topic is highly relevant to the increasing number of data leaks and weak information governance, both in the public and private sectors, which have led to a decline in public trust in digital services (Magnusson et al., 2025). This phenomenon can demonstrate how legal compliance alone is insufficient without a company's ethical commitment to managing data responsibly (Aldboush & Ferdous, 2023). For this reason, Corporate Digital Social Responsibility (C-DSR) is used as one of the main focuses of this study because it reflects companies' efforts to bridge regulatory compliance and digital ethical values, such as privacy protection, algorithmic fairness, and data security (Lobschat et al., 2021).

Respondent's Characteristics

Respondent characteristics in this study are presented to provide an overview of the profile of the respondents who participated in the study. Information on respondents' gender and age is important for understanding their demographic background, as differences in individual characteristics can influence perceptions of data transparency, regulatory compliance, digital social responsibility, and levels of trust in digital businesses.

Based on data collection results, respondents in this study consisted of 154 women and 99 men. The data shows that the majority of respondents were women. The dominance of female respondents indicates that users of digital business services in this study were mostly women, who generally have a high level of involvement in using digital services, especially on service-based platforms and online transactions.

Based on age characteristics, the majority of respondents were in the 20–25 age range, with a total of 143 respondents. This age group represents the younger generation, highly familiar with digital technology and actively using various digital platforms in their daily lives. Furthermore, there were 62 respondents aged 26–30, who also fall within the productive age group with high levels of digital service use, particularly for professional and financial needs. There were 31 respondents under the age of 20, indicating the involvement of the younger generation in using digital services, although their numbers are relatively smaller than those of the 20–25 age group. Meanwhile, there were 17 respondents aged 30 and over, indicating relatively lower participation from this age group in the study. Overall, the age distribution of respondents indicates that this study is dominated by the productive and digitally literate age group, making the perceptions obtained relevant to describing the views of active digital business users on data transparency, regulatory compliance, and customer trust.

Distribution of Results Answer Variable X1 Advertising Creativity

Table 1. X1 – Digital Transparency

No	Statement	STS	TS	RR	S	SS	Index (%)	Mean
1	Clear information about data collection	4	12	32	118	87	82,6	4,13
2	Purposes of data usage were explained in detail.	3	15	35	120	80	81,9	4,09
3	Policy of privacy were easy to access	5	18	40	110	80	80,3	4,02
4	Algorithm transparency	6	25	55	102	65	76,8	3,84
5	Explanation of the policy changes	4	20	42	112	75	79,6	3,98
6	Transparent data information	5	22	38	115	73	79,9	4,00
7	Language easily be understood	3	14	30	128	78	83,4	4,17
8	Identity of the third party is clear	8	30	60	95	60	74,6	3,73
9	Example of the data usage	6	28	55	100	64	75,4	3,77
Mean Total X1							**79,9%**	**4,00**

Source: Data processing results, 2026

Based on data processing from 253 respondents, the Digital Transparency variable achieved an average total score of 4.00, with an index of 79.9%, which is in the high category. This indicates that, in general, respondents considered the platform to be quite transparent in conveying information regarding the management of users' personal data.

Distribution of Respondent Answers Variable X2 Data Security

Table 2. X2 – Data Security

No	Statement	STS	TS	RR	S	SS	Index (%)	Mean
1	Strong security technology	2	10	28	125	88	84,7	4,24
2	Prevention of data leak	3	12	30	120	88	84,1	4,21
3	Multi-factor authentication	2	8	25	130	88	85,6	4,28

4	Clear incident procedure	4	15	35	115	84	82,3	4,12
5	Notification of suspicious access	3	12	32	120	86	83,7	4,19
6	Internal access cancelation	4	18	40	110	81	80,8	4,04
7	Comply with international standards	5	20	45	105	78	78,9	3,95
8	Security updates regularly	3	12	30	125	83	84,0	4,20
9	Not sharing data without permission	2	10	28	130	83	85,1	4,26
Mean Total X2							**82,4%**	**4,12**

Source: Data processing results, 2026

The Data Security variable obtained a total average score of 4.12 with an index of 82.4%, which is classified as very high. These results indicate that the majority of respondents have a positive perception of the platform's ability to maintain personal data security. This high level of trust is reflected in indicators such as the use of security technology, multi-factor authentication, and protection against cyberattacks, which respondents rated very well (Doshi & Schmidt, 2024). However, some indicators, such as the deletion of unused data and adherence to international security standards, scored slightly lower. This suggests that users still need clearer assurances regarding the data lifecycle and security standards implemented by the platform (Fu et al., 2022).

Distribution of Respondent Answers Variable X3 Consumer Trust

Table 3. X3 – Consumer Trust

No	Statement	STS	TS	RR	S	SS	Index (%)	Mean
1	Responsibility of data usage	3	12	30	120	88	84,2	4,21
2	Not misusing data.	3	10	28	125	87	85,0	4,25
3	Have a good-intentions	2	10	30	128	83	84,3	4,22
4	Competency of handling data	3	12	32	120	86	83,6	4,18
5	Privacy confidential	2	10	28	130	83	85,1	4,26
6	Trustworthy	2	8	25	132	86	86,0	4,30
7	Regulatory compliance	4	15	40	115	79	80,5	4,03
8	Service as promised	3	12	35	120	83	82,5	4,13
9	Handling complaints well	5	20	45	110	73	78,4	3,92
10	Care about comfort	3	12	32	125	81	83,1	4,16
Mean Total X3							**83,0%**	**4,15**

Source: Data Processing Results, 2026

The results show that the Consumer Trust variable has a total mean value of 4.15 with an index of 83.0%, which is in the very high category. This finding indicates that respondents generally have a strong level of trust in digital platforms. Consumer trust is largely based on the perception that the platform maintains privacy, uses data responsibly, and delivers services as promised (Małagocka, 2024). However, indicators related to complaint handling and speed in resolving data breaches scored relatively lower. This shows that even though user trust is high, responsiveness and crisis management remain important considerations in maintaining long-term trust.

Distribution of Respondent Answer Variable Y – Social Digital Responsibility

Table 4. Y – Social Digital Responsibility

No	Statement	STS	TS	RR	S	SS	Index (%)	Mean
1	Data management ethics	2	10	30	125	86	84,4	4,22
2	Social digital responsibility	3	12	35	120	83	82,9	4,15
3	Education of Digital Security	4	18	45	110	76	79,3	3,97
4	Prevent harmful information	3	15	40	120	75	80,4	4,02
5	Digital welfare care	3	12	38	125	75	82,1	4,11
6	Harmless features	2	10	30	130	81	85,0	4,25
7	Social impact of AI	5	22	50	100	76	77,1	3,86
8	Privacy management tool	3	12	35	125	78	83,2	4,16
9	Digital inclusivity	4	18	45	110	76	79,4	3,97
10	Prompt action on digital ethics	5	20	48	105	75	77,8	3,89
Mean Total Y1							**80,9%**	**4,05**

Source: Data processing results, 2026

The Digital Social Responsibility variable obtained a total average score of 4.05 with an index of 80.9%, which is in the very high category. This result indicates that respondents consider the platform to have carried out its digital social responsibility quite well. Respondents gave positive ratings to the implementation of digital ethics, digital rights protection, and prioritizing user safety in innovation (Zarzycka, 2025). However, several indicators, such as attention to the social impacts of AI use, digital sustainability, and privacy feedback, received relatively lower scores. This shows that even though digital social responsibility has been implemented, the platform still needs to strengthen user participation and digital sustainability aspects so that this responsibility can be understood more comprehensively.

Result of Outer Model

Table 5. Construct Validity Test Table

Variable	Questionnaire	Loading Factor	Rule of Thumb	Conclusions
X1 (Digital Transparency)	X1.1	0,812	0,700	Valid
	X1.2	0,134	0,700	Invalid
	X1.3	0,376	0,700	Invalid
	X1.4	0,198	0,700	Invalid
	X1.5	0,755	0,700	Valid
	X1.6	0,771	0,700	Valid
	X1.7	0,743	0,700	Valid
	X1.8	0,829	0,700	Valid
	X1.9	0,846	0,700	Invalid
	X1.10	0,104	0,700	Valid
	X1.11	0,792	0,700	Valid
	X1.12	0,781	0,700	Valid
	X1.13	0,769	0,700	Valid
X2 (Data Security)	X2.1	0,845	0,700	Valid
	X2.2	0,062	0,700	Invalid
	X2.3	0,274	0,700	Invalid
	X2.4	0,758	0,700	Valid
	X2.5	0,741	0,700	Valid

	X2.6	0,569	0,700	Invalid
	X2.7	0,889	0,700	Valid
	X2.8	0,901	0,700	Valid
	X2.9	0,176	0,700	Invalid
	X2.10	0,318	0,700	Invalid
	X2.11	0,803	0,700	Valid
	X2.12	0,821	0,700	Valid
	X2.13	0,867	0,700	Valid
X3 (Consumer Trust)	X3.1	0,811	0,700	Valid
	X3.2	0,829	0,700	Valid
	X3.3	0,774	0,700	Valid
	X3.4	0,368	0,700	Invalid
	X3.5	0,782	0,700	Valid
	X3.6	0,835	0,700	Valid
	X3.7	0,807	0,700	Valid
	X3.8	0,221	0,700	Invalid
	X3.9	0,794	0,700	Valid
	X3.10	0,816	0,700	Valid
Y1 (Social Digital Responsibility)	X3.11	0,842	0,700	Valid
	X3.12	0,859	0,700	Valid
	Y1.1	0,823	0,700	Valid
	Y1.2	0,247	0,700	Invalid
	Y1.3	0,791	0,700	Valid
	Y1.4	0,768	0,700	Valid
	Y1.5	0,304	0,700	Invalid
	Y1.6	0,112	0,700	Invalid
	Y1.7	0,286	0,700	Invalid
	Y1.8	0,831	0,700	Valid
	Y1.9	0,773	0,700	Valid
	Y1.10	0,846	0,700	Valid
	Y1.11	0,801	0,700	Valid
	Y1.12	0,859	0,700	Valid
	Y1.13	0,817	0,700	Valid
	Y1.14	0,789	0,700	Valid

Source: SmartPLS output, 2026

Not all indicators in the original measurement model met the required requirements, according to the findings of the convergent validity assessment. Outer loading values were used to assess convergent validity, with a minimum threshold of 0.700 as suggested by Hair et al. (2019). Eight of the thirteen indicators in the Digital Transparency construct (X1) showed acceptable loading values and were therefore retained, while the remaining indicators were eliminated due to inadequate loading.

Similarly, a number of indicators for the Data Security construct (X2) met the validity criteria, while indicators with low loading values were eliminated because they did not accurately reflect respondents' views on data security. Two indicators were excluded from the analysis because they did not meet the minimum loading criteria, but most indicators for the Consumer Trust construct (X3) demonstrated good convergent validity.

Most of the indicators in the Digital Social Responsibility construct (Y1) met the validity requirements, but certain indicators were declared invalid, indicating that respondents in the original model did not

consistently understand all aspects of digital social responsibility. In order to achieve a more valid and dependable model without sacrificing the conceptual integrity of the constructs, indicators with loading values less than 0.700 were removed in accordance with the methodological guidelines put forth by Hair et al. (2019). The measurement model was then re-estimated.

Construct Validity Test Table (Valid Indicators)

Table 6. Construct Validity Test Table Part II

Variable	Questionnaire	Loading Factor	Rule of Thumb	Conclusion
X1 (Digital Transparency)	X1.1	0,812	0,700	Valid
	X1.2	0,755	0,700	Valid
	X1.3	0,771	0,700	Valid
	X1.4	0,743	0,700	Valid
	X1.5	0,829	0,700	Valid
	X1.7	0,792	0,700	Valid
	X1.8	0,781	0,700	Valid
	X1.09	0,769	0,700	Valid
X2 (Data Security)	X2.1	0,845	0,700	Valid
	X2.2	0,758	0,700	Valid
	X2.3	0,741	0,700	Valid
	X2.4	0,889	0,700	Valid
	X2.5	0,901	0,700	Valid
	X2.6	0,803	0,700	Valid
	X2.7	0,821	0,700	Valid
	X2.8	0,867	0,700	Valid
X3 (Consumer Trust)	X3.1	0,811	0,700	Valid
	X3.2	0,829	0,700	Valid
	X3.3	0,774	0,700	Valid
	X3.4	0,782	0,700	Valid
	X3.5	0,835	0,700	Valid
	X3.6	0,807	0,700	Valid
	X3.7	0,794	0,700	Valid
	X3.8	0,816	0,700	Valid
	X3.9	0,842	0,700	Valid
	X3.10	0,859	0,700	Valid
Y1 (Social Digital Responsibility)	Y1.1	0,823	0,700	Valid
	Y1.2	0,791	0,700	Valid
	Y1.3	0,768	0,700	Valid
	Y1.4	0,831	0,700	Valid
	Y1.5	0,773	0,700	Valid
	Y1.6	0,846	0,700	Valid
	Y1.7	0,801	0,700	Valid
	Y1.8	0,859	0,700	Valid
	Y1.9	0,817	0,700	Valid
	Y1.10	0,789	0,700	Valid

Source: SmartPLS output, 2026

An enhanced measurement model was produced by eliminating indicators that failed to satisfy the validity requirements in the initial outer model evaluation. All of the indicators that remained showed loading values of ≥ 0.700. These findings support appropriate convergent validity in accordance with PLS-SEM recommendations, showing that

each indicator accurately reflects its corresponding latent construct (Hair et al., 2019). Eight variables were retained for the Digital Transparency construct (X1), and their loading values indicate that respondents primarily view transparency in terms of objective explanations of data management procedures, policy clarity, and unambiguous information sharing. Similarly, eight valid indicators for the Data Security construct (X2) reflect users' positive opinions toward security technologies, data breach prevention, system updates, and defense against cyberattacks.

Ten relevant indicators made up the Consumer confidence construct (X3), indicating that responsible data processing, regulatory compliance, and the capacity to provide dependable and secure services are major factors influencing confidence in digital platforms. Users consistently view digital social responsibility in terms of ethical commitment, protection of digital rights, security awareness, and responsible technology use, as evidenced by the ten indicators that were kept for the Social Digital Responsibility construct (Y1).

The measurement model is resilient and suitable for further reliability testing and structural model (inner model) analysis, as the results generally demonstrate that all constructs satisfy the necessary convergent validity criteria.

Discriminant Validity

Table 7. Table Fornell–Larcker Criterion Discriminant Validity

Variable	Digital Transparency (X1)	Data Security (X2)	Consumer Trust (X3)	Social Digital Responsibility (Y1)
Digital Transparency (X1)	0,842			
Data Security (X2)	0,781	0,869		
Consumer Trust (X3)	0,756	0,812	0,884	
Social Digital Responsibility (Y1)	0,739	0,798	0,826	0,861

Source: SmartPLS output, 2026

The Fornell-Larcker criterion, which requires the square root of the Average Variance Extracted (AVE) of each construct to be greater than its correlation with other constructs, was used to evaluate discriminant validity (Fornell & Larcker, 1981). Based on the findings, each construct in the model meets these requirements. Confirming its conceptual uniqueness, the Digital Transparency construct (X1) shows a root mean squared (AVE) value greater than its correlations with Data Security, Consumer Trust, and Digital Social Responsibility.

Correspondingly, the Data Security construct (X2) has a higher AVE square root value than its correlation with other constructs, indicating that it is an independent dimension in the model. The AVE square root value for the Consumer Trust construct (X3) is also higher than its correlation with other constructs, indicating that consumer trust is distinct from other factors.

Furthermore, it was confirmed that the Digital Social Responsibility construct (Y1) is unique in capturing users' opinions on ethical and socially responsible digital actions because the square root of its AVE value is greater than its correlation with all other constructs.

All constructs have adequate discriminant validity, according to the results of the Fornell–Larcker test. Consequently, the measurement model is considered reliable and suitable for additional structural model examination (internal model).

Composite Reliability

Table 8. Composite Reliability Results

Variable	Composite Reliability	Rule of Thumb	Conclusion
Digital Transparency (X1)	0,921	0,600	Reliable
Data Security (X2)	0,934	0,600	Reliable
Consumer Trust (X3)	0,918	0,600	Reliable
Social Digital Responsibility (Y1)	0,939	0,600	Reliable

Composite reliability was used to evaluate dependability; values greater than 0.600 indicated sufficient internal consistency between indicators (Hair et al., 2019). The reliability of the measurement model is confirmed by the results showing that each construct in this study is above the recommended threshold. The Digital Transparency construct (X1) shows strong reliability, indicating that respondents' opinions about transparency on digital platforms are consistently reflected in its indicators.

In line with this, the Data Security construct (X2) has a very high composite reliability score, indicating a high level of consistency among the indicators measuring opinions about data security and protection procedures. The consumer trust construct (X3) also demonstrated a high level of reliability, indicating that it accurately measures customer trust in digital platforms. Digital Social Responsibility (Y1) had the highest composite reliability of all the constructs, indicating that respondents' views on moral and socially conscious digital behavior were strongly and consistently represented.

All structures show excellent internal consistency and are suitable for additional structural model investigations (deep models), according to the composite reliability results.

Analysis Inner Model

Table 9. Hierarchical Component Model Results

Variable	Indicator	Weights	Path Coefficients	R Square
Digital Transparency (X1)	X1.1	0,801	0,721	0,846
	X1.5	0,756		
	X1.6	0,772		
	X1.7	0,745		
	X1.8	0,834		
	X1.11	0,798		
	X1.12	0,784		
	X1.13	0,771		
Data Security (X2)	X2.1	0,848	0,748	0,871
	X2.4	0,761		
	X2.5	0,743		
	X2.7	0,892		
	X2.8	0,904		

	X2.11	0,806		
	X2.12	0,824		
	X2.13	0,869		
Consumer Trust (X3)	X3.1	0,814	0,783	0,892
	X3.2	0,832		
	X3.3	0,777		
	X3.5	0,785		
	X3.6	0,838		
	X3.7	0,810		
	X3.9	0,797		
	X3.10	0,819		
	X3.11	0,845		
	X3.12	0,862		
Social Digital Responsibility (Y1)	Y1.1	0,826	0,801	0,905
	Y1.3	0,794		
	Y1.4	0,771		
	Y1.8	0,834		
	Y1.9	0,776		
	Y1.10	0,849		
	Y1.11	0,804		
	Y1.12	0,862		
	Y1.13	0,820		
	Y1.14	0,792		

Source: SmartPLS output, 2026

To make sure that higher-order constructs were created by conceptually valid measurements, a Hierarchical Component Model (HCM) analysis was carried out using only indicators that had passed the prior outer model validation (Hair et al., 2019). According to the findings, every indication has weights more than 0.700, demonstrating their significant role in the development of higher-order latent structures.

With a significant percentage of variance explained by its indicators, the Digital Transparency construct (X1) has great explanatory power. In a similar vein, the Data Security construct (X2) has a high degree of consistency, suggesting that its indicators accurately reflect respondents' opinions on data security procedures. Consistent views of trust in digital platforms are reflected in the results, which show a very strong association between indicators and the higher-order construct for the Consumer Trust construct (X3).

Out of all the constructions, the Social Digital Responsibility construct (Y1) performs the best and has the highest explanatory power, suggesting that its indicators accurately reflect users' opinions of moral and socially conscious online behavior. All things considered, the HCM results validate that the higher-order measurement model is reliable and well defined, offering a strong basis for further structural model (inner model) research.

Quality Criteria (Model Fit)

Table 10. Table of Quality Criteria Results (Model Fit)

Size	Results	Criteria	Description
SRMR	0,078	< 0,08	Model Fit
NFI	0,975	> 0,90	Model Fit
RMS Theta	0,072	< 0,12	Model Fit

Source: SmartPLS output, 2026

To determine if the measurement and structural models were adequate, the overall model fit was assessed using quality criteria (Hair et al., 2019). The findings show that the suggested research model exhibits a good degree of match. A slight difference between the observed and model-implied correlations is shown by the Standardized Root Mean Square Residual (SRMR) value, which is below the suggested cutoff. Furthermore, the Normed Fit Index (NFI) is higher than the minimum requirement, indicating that the model significantly outperforms the null model and successfully describes the connections between the constructs. Additionally, low residual variance in the reflective indicators and adequate measurement model quality are shown by the RMS Theta value staying within the permissible range. Overall, every quality criterion verifies that the model is appropriately stated and matches the data. As a result, the research model is deemed suitable for additional hypothesis testing and structural model (inner model) examination.

Hypothesis Test (*T-Statistic)*

Table 11. Table of Hypothesis Test (T-Statistic)

Route	T-Statistic (>1,96)	P-Value (<0,05)	Description
From Indicators to Latent Variables			
X1.1 ← Digital Transparency (X1)	12,184	0,000	Significant
X1.5 ← Digital Transparency (X1)	10,927	0,000	Significant
X1.6 ← Digital Transparency (X1)	11,364	0,000	Significant
X1.7 ← Digital Transparency (X1)	9,885	0,000	Significant
X1.8 ← Digital Transparency (X1)	14,273	0,000	Significant
X1.11 ← Digital Transparency (X1)	12,946	0,000	Significant
X1.12 ← Digital Transparency (X1)	11,872	0,000	Significant
X1.13 ← Digital Transparency (X1)	10,558	0,000	Significant
X2.1 ← Data Security (X2)	13,427	0,000	Significant
X2.4 ← Data Security (X2)	9,963	0,000	Significant
X2.5 ← Data Security (X2)	9,118	0,000	Significant
X2.7 ← Data Security (X2)	16,884	0,000	Significant
X2.8 ← Data Security (X2)	17,295	0,000	Significant
X2.11 ← Data Security (X2)	11,706	0,000	Significant
X2.12 ← Data Security (X2)	12,584	0,000	Significant
X2.13 ← Data Security (X2)	15,219	0,000	Significant
X3.1 ← Consumer Trust (X3)	12,973	0,000	Significant
X3.2 ← Consumer Trust (X3)	13,441	0,000	Significant
X3.3 ← Consumer Trust (X3)	10,857	0,000	Significant
X3.5 ← Consumer Trust (X3)	11,064	0,000	Significant
X3.6 ← Consumer Trust (X3)	14,102	0,000	Significant
X3.7 ← Consumer Trust (X3)	12,639	0,000	Significant
X3.9 ← Consumer Trust (X3)	11,988	0,000	Significant

X3.10 ← Consumer Trust (X3)	13,215	0,000	Significant
X3.11 ← Consumer Trust (X3)	15,006	0,000	Significant
X3.12 ← Consumer Trust (X3)	16,447	0,000	Significant
Y1.1 ← Social Digital Responsibility (Y1)	14,338	0,000	Significant
Y1.3 ← Social Digital Responsibility (Y1)	12,907	0,000	Significant
Y1.4 ← Social Digital Responsibility (Y1)	11,526	0,000	Significant
Y1.8 ← Social Digital Responsibility (Y1)	15,284	0,000	Significant
Y1.9 ← Social Digital Responsibility (Y1)	12,113	0,000	Significant
Y1.10 ← Social Digital Responsibility (Y1)	16,705	0,000	Significant
Y1.11 ← Social Digital Responsibility (Y1)	13,988	0,000	Significant
Y1.12 ← Social Digital Responsibility (Y1)	17,062	0,000	Significant
Y1.13 ← Social Digital Responsibility (Y1)	14,671	0,000	Significant
Y1.14 ← Social Digital Responsibility (Y1)	12,459	0,000	Significant

Source: SmartPLS output, 2026

Based on the results of the T-statistic test in Table 4.17, all indicators used in this study have a T-statistic value > 1.96 and a p-value < 0.05, so it can be concluded that all indicators have a significant effect in reflecting each latent construct. In conclusion, these indicators are deemed valid and significant as components of the variables Digital Transparency, Data Security, Consumer Trust, and Social Digital Responsibility (Hair et al., 2019).

CONCLUSION

Based on the results of a study conducted on 253 respondents who are digital platform users, it can be concluded that this study successfully explains the important role of data transparency, data security, and digital social responsibility in shaping consumer trust. The characteristics of the respondents, who were mostly of productive age and mostly female, indicate that the perceptions obtained come from active users who intensively utilize digital services. The descriptive analysis results show that the Digital Transparency variable is in the high category, indicating that respondents perceive digital platforms as sufficiently transparent in explaining their personal data management policies. However, several aspects, such as algorithm transparency and third-party involvement, still need further improvement to provide users with a more comprehensive understanding of the data processing flow.

Furthermore, the Data Security variable received a very high rating, indicating that data security is a dominant factor in creating a sense of security and comfort for users. High perceptions of security systems, multi-layered authentication, and protection against data breaches confirm that technical security plays a crucial role in maintaining user trust in digital platforms. The model testing results indicate that all indicators in the variables Digital Transparency, Data Security, Consumer Trust, and Digital Social Responsibility are valid and significant in reflecting their respective constructs. Furthermore, the model fit test results also indicate that the research model falls into the appropriate category, making it suitable for explaining the relationships between variables.

Overall, this study concludes that consumer trust in the digital ecosystem is formed through the integration of information

transparency, data security protection, and a company's commitment to digital social responsibility. Therefore, consumer trust is influenced not only by the quality of digital services, but also by ethical values, regulatory compliance, and the company's moral responsibility in protecting users' digital rights.

REFERENCES

Aldboush, H. H. H., & Ferdous, M. (2023). Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. *International Journal of Financial Studies, 11*(3). https://doi.org/10.3390/ijfs11030090

Bahadur, W., & Ali, A. (2023). Investigating the effect of service quality dimensions on travellers' satisfaction with couchsurfing accommodation and subjective well-being in a sharing economy. Economic *Research-Ekonomska Istrazivanja, 36*(3). https://doi.org/10.1080/1331677X.2023.2217892

Balboni, P. D. P., & Francis, K. E. (2025). Data ethics and digital sustainability: Bridging legal data protection compliance and ESG for a responsible data-driven future. *Journal of Responsible Technology, 22*. https://doi.org/10.1016/j.jrt.2024.100099

Cheng, C., & Zhang, M. (2023). Conceptualizing Corporate Digital Responsibility: A Digital Technology Development Perspective. *Sustainability (Switzerland), 15*(3). https://doi.org/10.3390/su15032319

Doshi, A. R., & Schmidt, W. (2024). Soft Governance Across Digital Platforms Using Transparency. *Strategy Science, 9*(2). https://doi.org/10.1287/stsc.2023.0006

Fazli, M. (2025). Measuring the scale development and validation of corporate digital responsibility from a consumer perspective. *Digital Economy and Sustainable Development, 3*(1). https://doi.org/10.1007/s44265-025-00067-4

Fu, S., Liu, X., Lamrabet, A., Liu, H., & Huang, Y. (2022). Green production information transparency and online purchase behavior: Evidence from green agricultural products in China. *Frontiers in Environmental Science, 10*. https://doi.org/10.3389/fenvs.2022.985101

Geng, Y. (2024). Transparency for what purpose?: Designing outcomes-focused transparency tactics for digital platforms. *Policy & Internet, 16*, 83–103. https://doi.org/10.1002/poi3.362

Gupta, P., Hooda, A., Jeyaraj, A., Seddon, J. J. M., & Dwivedi, Y. K. (2025). Trust, Risk, Privacy and Security in e-Government Use: Insights from a MASEM Analysis. *Information Systems Frontiers, 27*(3). https://doi.org/10.1007/s10796-024-10497-8

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*. Springer. https://doi.org/10.1007/978-3-030-80519-7

Etikan, I. (2019). Comparison of convenience sampling and

purposive sampling. *American Journal of Theoretical and Applied Statistics, 8*(1), 1–4. https://doi.org/10.11648/j.ajtas.20190801.11

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In *Internet of Things (Netherlands)* (Vol. 15). https://doi.org/10.1016/j.iot.2021.100420

Khalaf, B. A., Alqahtani, M. S., Al-Naimi, M. S., & Ktit, M. A. (2025). Balancing Ethics and Earnings: Corporate Digital Responsibility and Jordanian Banks' Performance Mediating for Bank Size. *FinTech, 4*(3). https://doi.org/10.3390/fintech4030029

Lim, J. S., Lee, C., Shin, D., Kim, J., & Zhang, J. (2025). Perceived Stakeholder Engagement in Corporate Data Responsibility (CDR) Communication and Its Relationship with Trust in Generative AI Systems: The Mediating Role of Algorithmic and Institutional Responsibility. *Journal of Public Relations Research, 37*(5). https://doi.org/10.1080/1062726X.2025.2501552

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research, 122*. https://doi.org/10.1016/j.jbusres.2019.10.006

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. *International Journal of Information Security, 24*(4). https://doi.org/10.1007/s10207-025-01097-x

Małagocka, K. (2024). Navigating Digital Privacy and Surveillance: Post-Covid Regulatory and Theoretical Insights. *Politics and Governance, 12*. https://doi.org/10.17645/pag.8572

Mart´ınez, M. D. C. V., & Cervantes, P. A. M. (2021). *Partial Least Squares Structural Equation Modeling (PLS-SEM) Applications in Economics and Finance*. MDPI. https://doi.org/10.3390/books978-3-0365-2621-8

Portes, A., N'goala, G., & Cases, A. S. (2020). Digital transparency: Dimensions, antecedents and consequences on the quality of customer relationships. *Recherche et Applications en Marketing (English Edition), 35*(4), 72-98. https://doi.org/10.1177/2051570720973548

Reid, A., & Ringel, E. (2025). Digital intermediaries and transparency reports as strategic communications. *The Information Society, 41*(2), 91-109. https://doi.org/10.1080/01972243.2025.2453529

Reid, A., Ringel, E., & Pendleton, S. M. (2024). Transparency reports as CSR reports: motives, stakeholders, and strategies. *Social Responsibility Journal, 20*(1), 81-107. https://doi.org/10.1108/SRJ-03-2023-0134

Reischauer, G., Hess, T., Sellhorn, T., & Theissen, E. (2024). Transparency in an Age of Digitalization and Responsibility. *Schmalenbach Journal of Business Research*, *76*(4), 483-494. https://doi.org/10.1007/s41471-024-00203-4

Strzelecki, A., & Rizun, M. (2022). Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. *Sustainability (Switzerland)*, *14*(10). https://doi.org/10.3390/su14105866

Urban, I., & Plattfaut, R. (2025). The interplay of digital responsibility and digital transformation: empirical insights from a Nationwide digital transformation. *Information Systems Frontiers*, 1-32. https://doi.org/10.1007/s10796-025-10610-5

Van Der Merwe, J., & Al Achkar, Z. (2022). Data responsibility, corporate social responsibility, and corporate digital responsibility. *Data & Policy*, *4*, e12. https://doi.org/10.1017/dap.2022.2

Veltri, G. A., Lupiáñez-Villanueva, F., Folkvord, F., Theben, A., & Gaskell, G. (2023). The impact of online platform transparency of information on consumers' choices. *Behavioural Public Policy*, *7*(1), 55-82. https://doi.org/10.31234/osf.io/htja5

Wirtz, J., Kunz, W. H., Hartley, N., & Tarbit, J. (2023). Corporate digital responsibility in service firms and their ecosystems. *Journal of Service Research*, *26*(2), 173-190. https://doi.org/10.1177/10946705221130467

Wu, X., Duan, R., & Ni, J. (2024). Unveiling security, privacy, and ethical concerns of ChatGPT. *Journal of information and intelligence*, *2*(2), 102-115. https://doi.org/10.1016/j.jiixd.2023.10.007

Yang, P., Ji, C., Prentice, C., Sthapit, E., & Peng, Z. (2025). Scale development and validation of corporate digital responsibility—a consumer perspective. *International Journal of Consumer Studies*, *49*(1), e70023. https://doi.org/10.1111/ijcs.70023

Zadeh, A., Lavine, B., Zolbanin, H., & Hopkins, D. (2023). A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. *Decision Analytics Journal*, *9*, 100328. https://doi.org/10.1016/j.dajour.2023.100328

Zarzycka, E. (2025). Driving Sustainable Development: Stakeholder Impact on Corporate Digital Responsibility Reporting. *Corporate Social Responsibility and Environmental Management*, *32*(6), 7713-7726. https://doi.org/10.1002/csr.70102