Mednarodno inovativno poslovanje
Journal of Innovative Business and Management

Trust in the age of artificial intelligence: a framework for privacy protection in personalised marketing

Maja Gorjanc*

Abstract: In the era of artificial intelligence (AI), first-party data is becoming a strategic asset for responsible and privacy-friendly personalization in marketing. This paper explores the ethical and legal aspects of AI-driven personalization through an integrated review of literature and empirical insights from the 2025 iPROM study on Slovenian companies' data practices. The key research question is: How does the level of data management maturity influence the perceived ethics of AI-driven marketing personalization? A trust-based conceptual framework is proposed, linking consumer perceptions of fairness, autonomy, and trust to organizational data governance practices. In Slovenia, fewer than half of companies (48.1%) currently show high technological maturity in data management, highlighting significant opportunities for improvement. There is clear potential to enhance digital empowerment by advancing data governance practices, adopting privacy-enhancing technologies (PETs), and strengthening regulatory compliance. The paper names key challenges and offers directions for developing responsible, consumer-centric AI personalization strategies.
Keywords: first-party data, personalization, consumer trust, privacy-enhancing technologies, artificial intelligence
JEL classification: M3, M31, M37

Maja Gorjanc*

**Faculty of social science, Ljubljana.*
DOBA Business School Maribor, Slovenia

maja.gorjanc@net.doba.si

DOI 10.32015/JIBM.2025.17.1.9

Mednarodno inovativno poslovanje = Journal of Innovative Business and Management

ISSN 1855-6175

Zaupanje v dobi umetne inteligence: okvir za varovanje zasebnosti pri personaliziranem marketingu

Povzetek: V dobi umetne inteligence (UI) postajajo prvoosebni podatki strateško pomembno orodje za odgovorno in zasebnosti prijazno personalizacijo v marketingu. Prispevek raziskuje etične in pravne vidike personalizacije, podprte z UI, na podlagi pregleda literature in empiričnih spoznanj iz raziskave iPROM (2025) o ravnanju slovenskih podjetij s potrošniškimi podatki. Ključno raziskovalno vprašanje je: Kako zrelost upravljanja s podatki vpliva na zaznano etičnost personalizacije marketinga z uporabo umetne inteligence? Predstavljen je konceptualni okvir, ki temelji na zaupanju in povezuje zaznavo potrošnikov glede pravičnosti, avtonomije in zaupanja s praksami upravljanja podatkov v podjetjih. V Sloveniji ima manj kot polovica podjetij (48,1%) visoko stopnjo tehnološke zrelosti pri upravljanju podatkov, kar kaže na pomemben potencial za izboljšave. Obstaja priložnost za večjo digitalno opolnomočenost podjetij, predvsem z razvojem naprednih praks upravljanja podatkov, uporabo tehnologij za varovanje zasebnosti (PET) in krepitev skladnosti z zakonodajo. Članek izpostavlja ključne izzive in predlaga usmeritve za razvoj odgovornih, k potrošniku usmerjenih strategij personalizacije z uporabo UI.
Ključne besede: prvoosebni podatki, personalizacija, zaupanje potrošnikov, tehnologije za varovanje zasebnosti, umetna inteligenca

INTRODUCTION

In a data-intensive, challenging environment, digital marketing is increasingly leveraging data through the integration of artificial intelligence (AI). The latter allows companies not only to better understand the customer, but also to target them more effectively. In the digital ecosystem, companies are slowly moving away from personalization based solely on the use of third-party data and are increasingly relying on the use of their own first-party data. The latter are becoming a key strategic resource as regulatory pressures increase (iPROM, 2025). This shift is not just a technological change but stands for a new paradigm in how organizations understand trust, transparency, and customer relationships (Martin & Palmatier, 2019).

The use of AI enables unprecedented levels of personalization and operational efficiency, but it also raises fundamental questions about data ownership, consumer autonomy, and algorithmic bias (Quach et al., 2022). Companies are at a crossroads: on the one hand, they need to use AI technology to optimize marketing outcomes, but on the other hand, they need to maintain ethical use of data and respect customer privacy (Nwobodo, 2025).

Drawing on the empirical research of iPROM company, a leading Slovene ad-tech provider with its own research Lab, and the expert and academic findings of various authors, the aim of this paper is to develop a comprehensible conceptual framework that introduces ethical, trust-based personalization into data-driven marketing. The goal is to explore how strategies for using first-party cues and AI technologies intersect with consumer trust, Privacy Enhancing Technologies (PETs), and the regulatory environment, and how together they shape marketing effectiveness in the era of digital accountability (Davenport et al., 2020).

1 LITERATURE REVIEW AND THEORETICAL BACKGROUND

The research process is based on a review of academic and practitioner literature focused on the use of undercurrents in marketing, artificial intelligence, privacy, ethical data management, and trust in digital marketing. Academic articles were selected based on their relevance to emerging trends in the use of first-party data, personalization with artificial intelligence, privacy-enhancing technologies, and regulatory compliance. The literature review provided a theoretical basis for the development of a conceptual framework that emphasizes trust, fairness, and perceived autonomy as central elements related to data use, technology, and marketing performance.

2 METHODOLOGY

A conceptual-empirical hybrid approach was used to design the paper, combining a structured literature review and an empirical industry survey. By combining theoretical and empirical sources, we developed a conceptual and strategic framework focused on ensuring customer trust that reflects both normative expectations and the realities of marketing practice.

2.1 iPROM empirical study on first-party data management in Slovenia

iPROM conducted an empirical study between August and October 2024; the author of the paper was part of the research team. The study is based on an unstructured, purposive sample of 66 marketing decision makers in Slovenian companies with direct experience in data strategy and digital marketing. The questionnaire included both closed and open-ended questions, and responses were collected through an online survey.
The content of the study focused on the transition of Slovenian companies from third-party data to first-party data strategies, the use of first-party data collection tools and privacy enhancing technologies, and the importance of legal compliance and alignment with GDPR and other regulations. Respondents also rated the maturity of data governance in their organizations. These empirical findings helped to frame and contextualize related concepts.

2.2 Additional industry insights and practical examples

In addition to the literature review and empirical study, this paper also includes the latest industry reports and examples. These additional sources support the formulation of theoretical categories and shed light on the practical challenges that digitally responsible companies face daily in establishing coherent and trustworthy personalization approaches using AI.
All methodological elements form an interdisciplinary basis and come together to form the framework proposed in this paper.
It is a simplified conceptual framework that can serve as a clear guide for companies that want to be ethical and digitally responsible and seek to apply ethical personalization marketing practices in the age of artificial intelligence.
Although the framework is theoretically grounded and empirically supported, it is a conceptual proposal that requires further validation. Therefore, we conclude the paper with a series of additional research suggestions that serve as directions for future empirical validation and theoretical extensions

3 THEORETICAL BACKGROUND AND GLOBAL TRENDS IN DATA MANAGEMENT

3.1 The rise of the importance of first-party data

First-party data is digital information that companies collect directly from their customers or users through their own digital platforms - such as websites, apps, online stores, CRM systems, and email. This data is considered highly accurate, dependable, and properly collected in compliance with privacy regulations. (iPROM, 2025) It is for tracking purposes that the data is increasingly used, as it is becoming a safer alternative to third party data and is slowly becoming cheaper in the context of personalized marketing. The iPROM survey (2025) shows that 75.4% of Slovenian companies already recognize the importance and value of first-party data; 56.8% of the companies surveyed already implement first-party data strategies and systems to manage this valuable proprietary data. Similarly, different whitepapers from large, globally successful companies that play an important role in digital capitalism - such as Shopify (2024) and Google (Google & IPSOS, 2020) - also confirm this trend, suggesting that first-party data is the foundation of a legally compliant personalized marketing strategy.

3.2 First-party data as a strategic asset in the digital economy

Xu et al. (2024) define data as a strategic asset and emphasize that for data to be valuable, it must be systematically collected, managed, and used in line with organizational goals. The authors describe a three-step process of data "asetization": (1) ensuring legal and technical readiness, (2) building organizational capacity, and (3) using data for strategic decision-making and innovation. The effective transformation of data into an asset requires not only the use of right technology infrastructure, skills and talent, but also ethical and regulatory awareness of how to manage that data. Their model makes an important contribution to defining the theoretical underpinnings of data governance. It also offers some practical guidelines for organizations looking to create long-term value from data.

3.3 Data science in personalised marketing

Based on the publications of Alwabel & Fatunmbi (2024) and iPROM (iprom.si, 2025), we define the basics of personalized marketing with the use of AI, from algorithms to AI models and tools used for personalization:

Centralized data collection
Data collection and integration involves aggregating customer data from multiple digital touchpoints, such as websites, social networks, and email. Centralized integration allows for more comprehensive analysis (Alwabel & Fatunmbi, 2024).

Customer segmentation
Customer segmentation is performed using clustering algorithms, which allow companies to target specific groups of consumers more effectively (Alwabel & Fatunmbi, 2024).

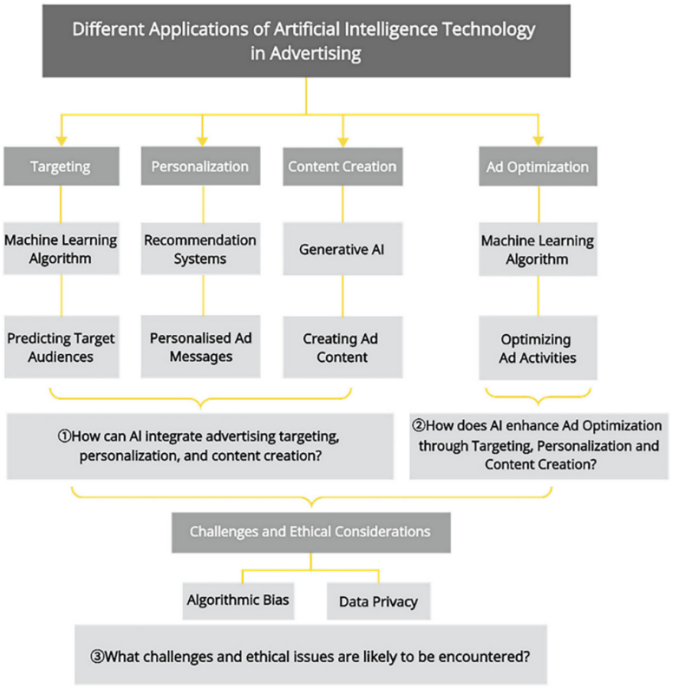
Predictive analytics
Predictive analytics allows companies to expect future customer behaviour (e.g., predicting future needs and purchases) and provide prompt, relevant marketing responses in the form of initiative-taking marketing (automated emails, remarketing with ads, etc.). Such automated recommendation systems use data methods to personalize products and the communication itself, further improving the user experience and increasing conversion potential (Alwabel & Fatunmbi, 2024).

Natural language processing (NLP)
NLP using artificial intelligence allows companies to extract valuable insights from customer feedback and opinions collected through various channels. This helps companies tailor marketing content to the real needs and challenges of customers (Alwabel & Fatunmbi, 2024).

Dynamic creative optimization
Dynamic Creative Optimization is a digital advertising technology that allows companies to automatically tailor your ad content to individual users in real time. It uses artificial intelligence and machine learning to analyse first-party data (e.g., location, behaviour, interests, past purchases) to create the most relevant version of an ad with dynamic elements - such as images, text, calls to action (CTAs), and pricing (iPROM, Real-time creative, 2025).

These data science techniques are the building blocks of dynamic and personalized marketing strategies.
AI is increasingly used in advertising for targeting, personalization, content creation, and ad optimization. By analysing consumer behaviour, AI provides insights that improve ad strategy, processing efficiency, and decision-making. In targeting, machine learning enhances online ad precision and audience segmentation (Gao et al., 2023).
The authors also developed a theoretical framework for AI in advertising, grounded in computational advertising which comprehensively integrates different AI technology methods into advertising (See Figure 1).

Figure 1: Different Applications of Artificial Intelligence Technology in Advertising (Gao et al., 2023)



Source: Gao, B., Wang, Y., Xie, H., & Hu, Y. (2023). Artificial intelligence in advertising: Advancements, challenges, and ethical considerations in targeting, personalization, content creation, and ad optimization

Targeting primarily uses machine learning to accurately find and reach the audience most likely to engage with an ad. Personalization relies on tools such as recommendation systems and virtual assistants to deliver tailored, relevant content to individual users. Content creation employs generative AI and natural language processing to produce engaging and creative material. Finally, ad optimization applies deep learning and reinforcement learning to continuously refine ad strategies, enhancing performance and return on investment (Gao et al., 2023).

3.4 Trust and fair use of data

Trust is a key mediator between data-driven personalisation and consumer acceptance of it. Quach et al. (2022) and Martin & Palmatier (2020) point out that consumers often do not know how their data is being used, leading to the so-called privacy paradox. This concept refers to the gap between expressed privacy concerns and actual user behaviour.
Kennedy et al. (2024), alongside the concept of trust, highlight the concept of fairness, which is also linked to the use of data. They find that users' perception of fairness is intricately linked to non-discriminatory use of data and to a sense of a balanced exchange of value between users and companies.
In the case of organisations, customer trust in them correlates strongly with legal compliance and transparent data use (e.g. explicit consent). iPROM's research (iPROM, 2025), for example, found that organisations with higher technological maturity also show stronger legal compliance and responsible handling of data, further underlining the importance of clear internal governance for building trust. iPROM's research also found that organisations with higher technological maturity show stronger legal compliance and responsible handling of data, further underlining the importance of clear internal governance for building trust. At this point, setting up a framework is logical as it offers clear direction and structure.

3.5 Ethics and trust in AI systems

AI technologies improve marketing through dynamic content personalization, predictive analytics, emotion recognition, and real-time customer interaction. Davenport et al. (2020) and Singla et al. (2023) describe how AI increases return on investment (ROI) and relevance to consumers by automating decision making throughout the purchase journey. In such cases, the line between technological sophistication to identify needs and the use of technology to manipulate the customer is extremely thin. It is therefore important to be aware that such systems often risk crossing ethical boundaries - especially when personalization becomes intrusive or emotionally manipulative.
Da Bormida (2022) points out that while the massive use of big data analytics, artificial intelligence, and predictive technologies offers transformative potential, it also introduces significant ethical and social risks into the whole discourse. This dynamic reflects the increasing "datafication" of society, with predictive technologies running at unprecedented speed and scale. This includes automated decision making and profiling, which can lead to discrimination, "social cooling" (i.e. reduced freedom of behaviour), and erosion of individual privacy. All this underscores the need for ethical frameworks, transparency and user-centred data governance that can serve as a counterbalance to the informational and systemic power asymmetries in the data-intensive economy and reduce the trust deficit in both the private and public sectors.

Trust in AI systems stems from their trustworthiness, ethical consistency, and integrity in use (Chen et al., 2024). Therefore, AI-based personalization is most effective when coupled with transparency and user control. This is because it allows for a balance between technological potential and ethical responsibility.

3.6 Privacy enhancing technologies and the regulatory environment

Global privacy legislation is becoming the cornerstone of digital business. Among the most influential pieces of legislation is the General Data Protection Regulation (GDPR), a European Union regulation that sets strict rules for the processing of personal data (Romansky & Noninska, 2020).

Artificial intelligence (AI) legislation is also in the pipeline, which will complement existing data protection regulations. The European Union has taken the most comprehensive approach in this regard with the AI Act, which is currently in the legislative process. This legislation aims to establish a

framework for the safe, transparent, and humane use of AI systems. However, efforts to harmonize AI regulation globally remain fragmented and uncoordinated. This creates challenges for companies working across borders and increases the importance of regulatory flexibility and advance compliance with technology-neutral privacy principles (EY, 2023). Compliance is no longer a choice, but a strategic imperative. All this is leading to the introduction of new technological protocols and direct consent data collection as a solution to enable personalization without violating privacy.

Privacy enhancing technologies (PETs) reduce legal risks and increase transparency and accountability of organizations. This already makes them a key component of the future of AI-powered marketing (Martin & Palmatier, 2020).

The development of PETs allows marketers to keep personalization capabilities while complying with strict privacy laws. For example, federated learning allows machine learning models to be trained on multiple devices or servers that store local data patterns - without sharing the actual data. Differential privacy introduces algorithmic noise into data sets to prevent individuals from being identified. These innovations not only meet regulatory requirements, but also help marketers build trust by using first-party data in a transparent and ethical way (Martin & Palmatier, 2020). As both regulators and consumers today demand more accountability, PETs are becoming indispensable tools in AI-driven marketing strategies.

4 RESEARCH PROPOSITIONS

Based on the literature review and the definition of basic concepts and theoretical frameworks, we defined the following research question: How does the level of data management maturity influence the perceived ethicality of digital marketing personalization?

Additionally, more in depth problem prepositions are explicitly formulated below and further addressed in the discussion section of this paper.

P1: Organizations that use technology to protect and manage their own data are more likely to build consumer trust in data-driven personalization supported by artificial intelligence.

P2: A higher level of maturity in managing organization's own first-party data has a positive impact on perceived fairness and transparency.

P3: First-party data strategies improve marketing return on investment (ROI), especially when combined with ethical data handling practices.

P4: Legal compliance mechanisms increase the credibility of personalization strategies in the eyes of customers and clients.

In the following sections, we will also highlight the practical and broader societal implications for the development of digitally responsible, consumer-centric, first-party personalization marketing strategies using AI.

5 EMPIRICAL FINDINGS ON FIRST-PARTY DATA MANAGEMENT IN SLOVENIA

The empirical basis of this paper is derived from the research report “Protecting Companies' Own Data and the Shift to First-Party Data Strategies in Digital Advertising”, conducted by iPROM between September and October 2024 and based on an online survey.

The survey involved 66 decision makers from digital marketing, advertising, and data management in Slovenian companies. The aim of the survey was to gain insights into current data use practices, challenges, and readiness of companies to use first-party data, follow legislation, and harness the potential of advanced technologies (iPROM, 2025).

The research report offers detailed insights into how companies are moving from strategies based on the use of third-party marketing feeds to first-party data strategies, and the extent to which companies are implementing data governance and compliance mechanisms.

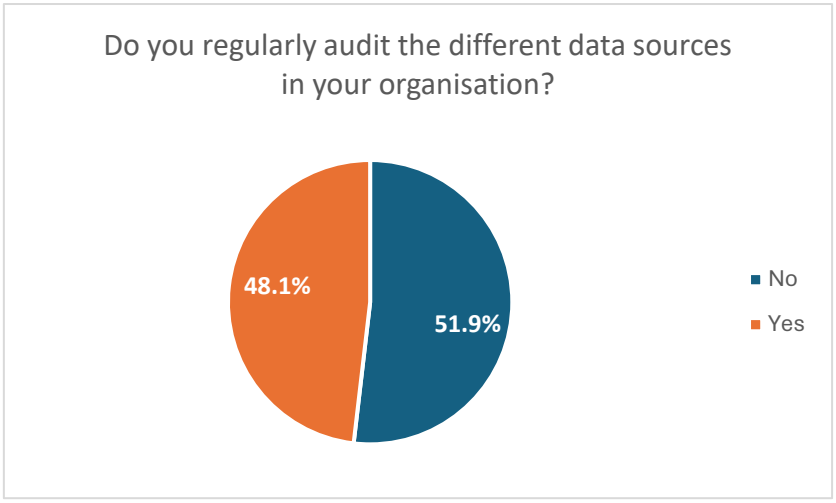
The sample size (66) is modest and exploratory; findings should be interpreted accordingly. In addition, the sample is limited to Slovenian companies, which may affect the generalizability of results.

5.1 Regular data audits

Almost half of Slovenian companies (48.1%) already conduct data audits (Figure2), which shows a positive trend in awareness of the importance of controlling data sources (iPROM, 2025).

At the same time, more than half of the companies (51.9%) still have room for improvement in this area. By continuing to invest in the right tools and processes to better manage data, companies could improve data quality and improve their data strategies (Figure 3).

Figure 2: Data Source Auditing in Organizations



Source: iPROM (2025). Protecting Companies' Own Data and the Shift to First-Party Data Strategies in Digital Advertising

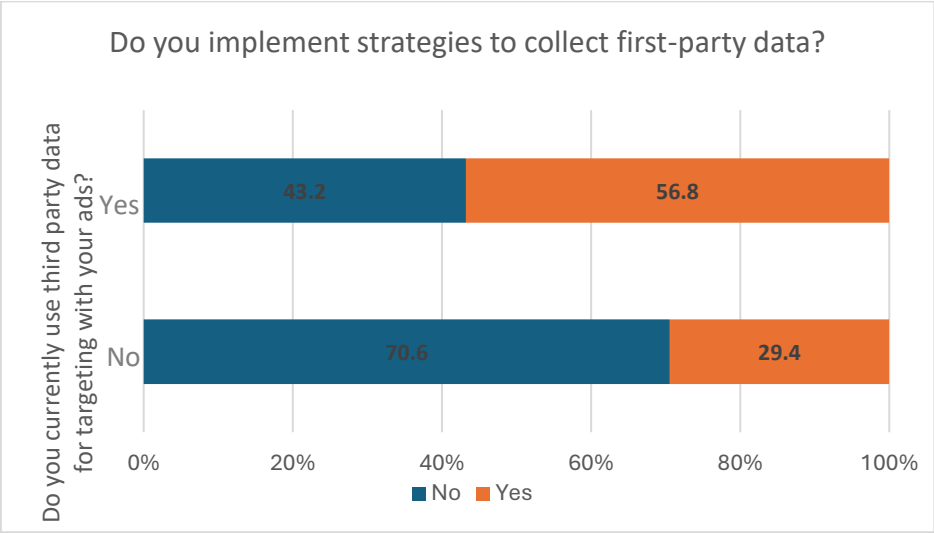
5.2 Recognition of first-party data as a strategic asset

More than half (56.8%) of Slovenian companies that use third-party data already have strategies in place to collect first-party data to improve marketing activities and ensure GDPR compliance.

However, 43.2% of these companies do not yet collect first-party data, which may reflect technical limitations or a lack of information and offers an opportunity for improvement.

Despite the heavy reliance on third party data (72.7%), there is a clear trend towards internal control of data, driven by regulatory pressure and the desire for better personalisation (iPROM, 2025).

Figure 3: The Use of First-Party and Third-Party Data for Personalization



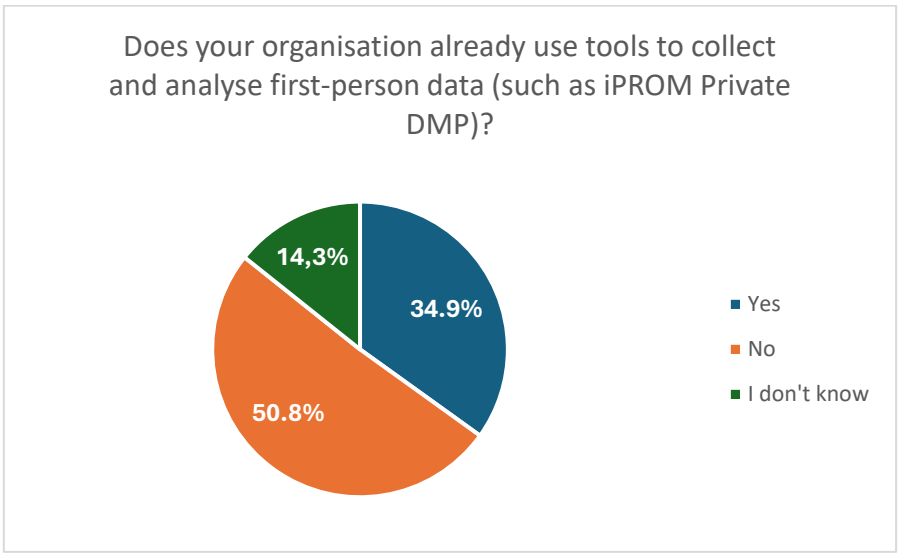
Source: iPROM (2025). Protecting Companies' Own Data and the Shift to First-Party Data Strategies in Digital Advertising

5.3 Adoption of privacy-enhancing technologies

A considerable proportion of Slovenian companies (34.9%) are already using advanced tools to collect and analyse first-party data (privacy-enhancing technologies), while 50.8% have not yet implemented such technologies.

This suggests an opportunity for more training and infrastructure development to support responsible data use and digital empowerment (iPROM, 2025).

Figure 4: Use of privacy enhancing technologies



Source: iPROM (2025). Protecting Companies' Own Data and the Shift to First-Party Data Strategies in Digital Advertising

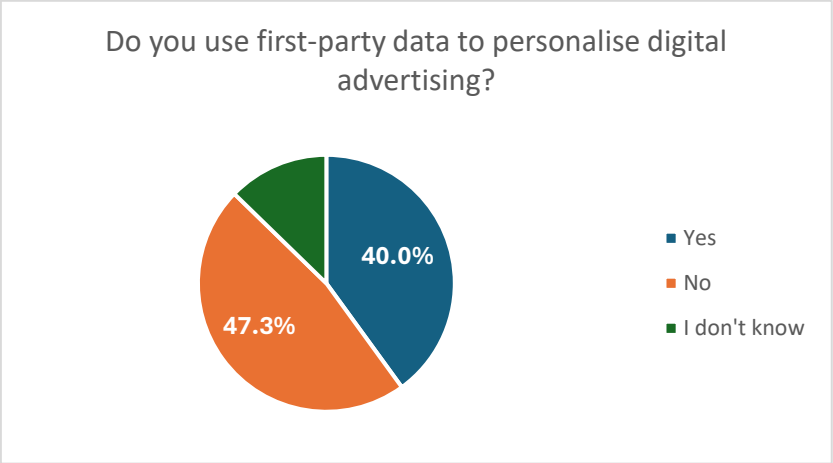
5.4 Use of first-party data for personalization

Almost half of companies (47.3%) do not yet use first-party data for personalization, being a missed opportunity for more effective and targeted advertising.

On the other hand, 40% are already using this valuable data, showing a shift towards more tailored, personalized campaigns.

12.7% of companies are unsure, highlighting the need for further education and awareness of the benefits of personalization based on first-party data (iPROM, 2025).

Figure 5: Use of first-party data for personalized advertising

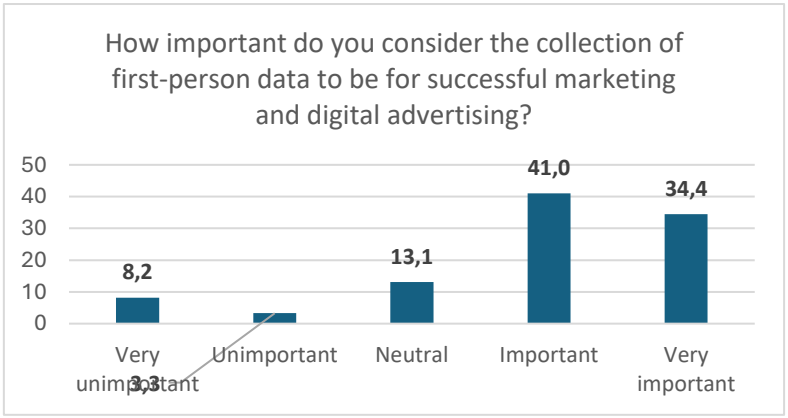


Source: iPROM (2025). Protecting Companies' Own Data and the Shift to First-Party Data Strategies in Digital Advertising

5.5 Strategic importance of first-party data

75.4% of respondents consider first-party data to be important or especially important to the success of digital advertising, with many citing better targeting, more effective campaigns, and reduced legal risk as key benefits.
Companies using first-party data strategies are also more likely to invest in audience activation and personalized advertising (iPROM, 2025).

Figure 6: Importance of first party data for personalised marketing



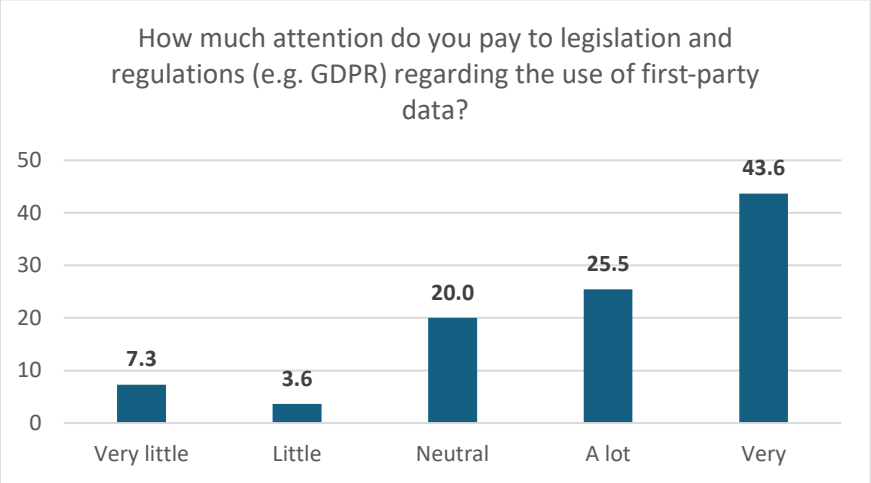
Source: iPROM (2025). Protecting Companies' Own Data and the Shift to First-Party Data Strategies in Digital Advertising

5.6 Focus on legal compliance

Most companies (69.1%) pay a great deal or very great deal of attention to compliance, showing a strong level of awareness of the importance of data protection.

Additionally, 68.9% of respondents confirmed that their organizations verify the compliance of their data partners, showing a broader shift towards a responsible and transparent data ecosystem (iPROM, 2025).

Figure 7: Importance of compliance regarding first party data usage



Source: iPROM (2025). Protecting Companies' Own Data and the Shift to First-Party Data Strategies in Digital Advertising

5.7 Overall trends

Overall, the results underline a clear shift towards the empowerment of Slovenian businesses in a digital-intensive economy. First-party data is becoming not only a privacy-friendly alternative but also a core strategic asset.

Figure 8: Company data maturity overview

Company data maturity	Share	Key data privacy practices
High maturity	48.1%	Regular data audits, use of PETs, compliance checks
Medium maturity	34.9%	Some privacy tools integrated, partial data audits
Low maturity	17.0%	Ad hoc practices, low compliance awareness

Source: iPROM (2025). Protecting Companies' Own Data and the Shift to First-Party Data Strategies in Digital Advertising

The varying levels of data maturity illustrate a growing segmentation in organizational capabilities. High-maturity companies (48.1%) are leading in responsible data governance and trust-based personalization. Medium-maturity firms (34.9%) are progressing but still face gaps, while low-maturity firms (17%) remain at risk due to insufficient compliance practices.

This maturity gradient underscores the importance of advancing data governance as a foundation for trustworthy AI-driven marketing, providing a basis for the conceptual framework developed in the following section.

6 ANALYSES

6.1 Digital empowerment and ethical models

Both iPROM's research and other sources (Quach et al., 2022) refer to the concept of digital empowerment of companies. This refers not only to data ownership as a fundamental value but also to the awareness of companies to manage this data in a transparent and responsible way.

Quach et al. (2022) propose an interesting typology of data governance, classifying companies into four main categories:

(I) Data harvesters are companies that aggressively collect and use data without much emphasis on transparency or consent.
(II) Patrons are companies that offer benefits to users in exchange for data.
(III) Informers are companies that try to inform consumers as much as possible about how they use data.
(IV) Experts are companies that demonstrate a high level of ethical awareness, transparency, and privacy.

This classification reflects companies' attitudes toward data sharing and monetization and is linked to their approach to ethical governance.
Similarly, iPROM (2025) finds that companies that use first-party data and regularly check the compliance of their data partners often demonstrate a more transparent and consumer-friendly approach. This supports the view that ethical as well as legal data governance is both a value system and a competitive advantage.
While data harvesters are digitally empowered but not digitally accountable, informers and experts are categories for whom accountability is key — not only at the level of providing basic information about data usage but also in ensuring the highest standards of privacy and trust.
In what follows, we propose a framework to guide companies that want to position themselves publicly as data professionals — digitally empowered and accountable — by proving a prominent level of ethical awareness, transparency, and data protection.
The proposed framework therefore combines different dimensions: technological, business, ethical, and regulatory. It provides a foundation for understanding how first-party data strategies and the use of artificial intelligence can influence marketing outcomes and the perception of a company or brand.

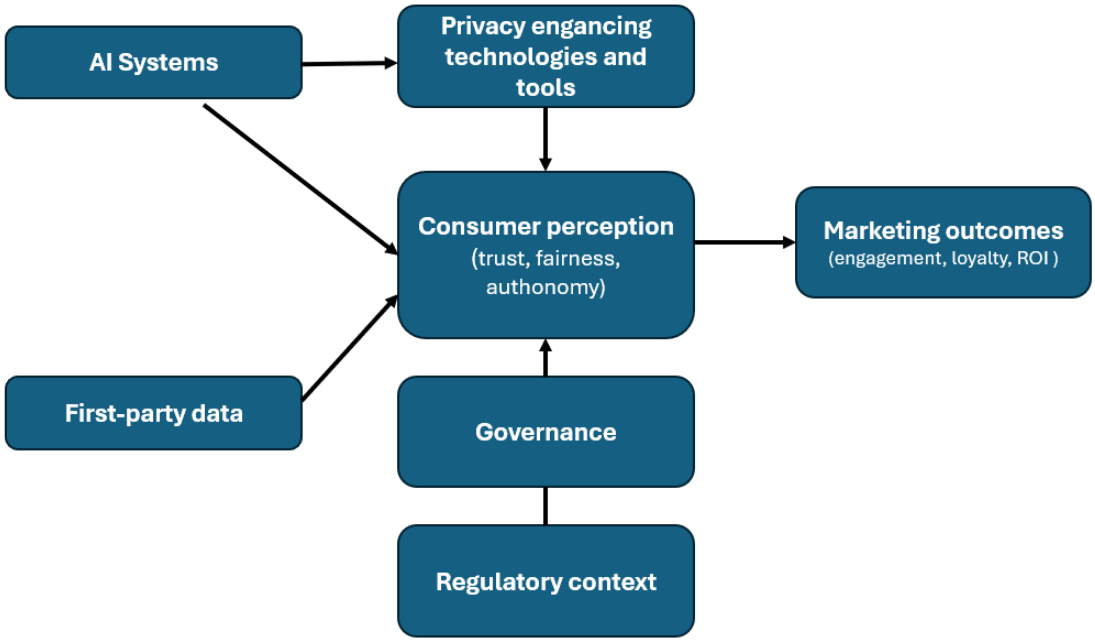
6.2 A conceptual framework for first-party data management using AI

This paper proposes a trust-focused framework that combines technological, ethical, and psychological perspectives to better understand how AI-powered personalization strategies work in the evolving data economy (Martin & Palmatier, 2020).
The framework highlights that marketing success increasingly depends not only on technical capabilities but also on how consumers perceive autonomy, fairness, and transparency in data handling.

It is a straightforward framework focused on trust (customer perceptions), capturing the interlinkages between first-party data strategies, artificial intelligence and related technologies, consumer perceptions, and marketing outcomes — all within a broader regulatory and technological context.
The framework (Figure 9) draws on insights from:

1. Empirical research by iPROM (2025),
2. Literature in marketing, privacy, and the ethics of AI use (Martin & Palmatier, 2019; Da Bormida, 2022; Davenport et al., 2020),
3. The author's experiential insights from collaborating with companies in marketing and digital marketing.

Figure 9: Conceptual Framework for First-party Data, AI, Ethical Governance and Marketing Efficiency



The framework is based on the premise that the ethical use of data, guided by the principles of fairness, transparency, and data sovereignty, directly impacts consumer trust (Da Bormida, 2022). Key elements of the framework are:

1. Consumer perception
Consumer perception refers to how individuals interpret and evaluate an organization's actions, policies, and communication about the handling of personal data. It is shaped by the level of transparency, clarity, and consistency in data practices, as well as by prior experiences, media coverage, and social influence. When consumers perceive that an organization acts ethically, respects privacy, and follows data protection regulations, their perception tends to be positive, hence reinforcing trust and engagement. (Yadav et al., 2024).

2.Privacy-enhancing technologies (PETs)
Privacy-Enhancing Technologies are digital tools and methods designed to enable data collection, processing, analysis, and sharing while preserving confidentiality and minimizing the exposure of personal information. PETs such as data obfuscation (e.g., anonymization, pseudonymization, synthetic data), encrypted processing (e.g., homomorphic encryption), federated analytics, and accountability mechanisms support compliance with privacy regulations and allow useful data utility without compromising individual privacy (OECD, 2023).

3.Regulatory context
Many regions have stringent data protection regulations, such as ZVOP-2 in Slovenia, the GDPR in Europe, CCPA in California and LGPD in Brazil, could broaden the view. Compliance with these regulations is not only a legal requirement but also a demonstration of an organization's commitment to data privacy (iPROM, 2025; Yadav et al., 2024)

4.Company governance
To achieve regulatory compliance, companies must strengthen internal data governance by setting up clear responsibilities, standardizing data practices, and ensuring transparency in data flows. Embedding privacy into system design and regularly monitoring data handling processes helps minimize risks and ensures alignment with legal obligations. Strong governance not only ensures compliance but also builds long-term trust. iPROM (2025)

At the heart of this framework is consumer perception comprising trust, fairness, and autonomy (the decision to share or consent to data use). This perception acts as a key mediator between technical resources and the strategic inputs and marketing outputs of organizations.

The framework suggests that companies that use first-party data effectively can improve ROI, engagement, and customer loyalty with AI, but only if they simultaneously implement responsible data management models and PET that support consumer trust.

Finally, the framework illustrates the shift from viewing data as a mere input for optimizing marketing to understanding data as a fundamental relational asset, where trust and ethics are key to long-term effectiveness.

Organizations are thus seen as active agents who must carefully balance technological opportunities and normative constraints, with responsible data management and PET adoption becoming essential components of modern marketing strategies.

7 DISCUSSION

7.1 The role of privacy technologies and the impact on trust

This section addresses P1: Organizations that use technology to protect and manage their own data are more likely to build consumer trust in data-driven personalization supported by artificial intelligence.
The key research propositions presented in this paper highlight those technologies such as PETs are more than just compliance tools — they actively shape consumer perceptions.
By implementing transparent data policies, continuously auditing data usage in the organization, and empowering users to manage their data through explicit consent, organizations can build lasting relationships based on trust (iPROM, 2025).
At the same time, it is important that personalization in marketing stays balanced. Excessive automation or behavioural targeting can reduce users' sense of autonomy, while too little personalization can reduce message relevance.
Future personalization strategies should go beyond mere compliance and implement systemic frameworks for data sharing that enable autonomy, negotiation, and trust, as suggested by Perko (2023).
If AI-powered agents (Gao et al., 2023) become more prevalent in marketing, user perception must be addressed by integrating AI agents into transparent and user-centred data management systems.

7.2 Trust, fairness, and exclusion in relation to personalization

This section addresses P2: A higher level of maturity in managing organization's own first-party data has a positive impact on perceived fairness and transparency.
Personalization based on first-party data offers strong marketing potential but can also exacerbate inequalities if used irresponsibly.
Certain group, such as the elderly, marginalized, or low-income individual, may lack access to digital devices or choose not to share data. This can lead to exclusion from personalized services.
Algorithms may also engage in commercial discrimination, withholding offers or content from users deemed less profitable. This raises ethical questions: Should market experiences be reserved only for algorithmically favoured profiles?
The future of responsible personalization requires a shift from maximizing efficiency to designing inclusive digital experiences. Companies must integrate ethical responsiveness and consumer psychology into their personalization strategies, building on the concept of digital maturity.
This perspective connects marketing technology, normative compliance, and user-centred ethics offering a holistic view of personalization. t also opens new avenues for research in user experience, behavioural economics, and trust in AI systems.

7.3 Practical applications of ethical governance of first-party data

This section addresses P3: First-party data strategies improve marketing return on investment (ROI), especially when combined with ethical data handling practices.
First-party data should be seen not only as a strategic asset but also as a cornerstone of ethical user engagement. Organizations adopting privacy technologies and investing in user-centric consent management platforms can gain a competitive advantage (Xu et al., 2024).

For example, companies such as Apple and iPROM (with their PET-enhancing product iPROM Private DMP) illustrate how privacy by design can be integrated into brand identity and become a market differentiator.
In addition to technical infrastructure, organizations must invest in data quality and interdisciplinary expertise (Xu et al., 2024). Moreover, data ethics should not be seen as a regulatory burden but as an integral part of brand identity and customer relationship strategy (Da Bormida, 2022).

Ethical oversight, internal audits, and agile governance models are key for companies working across multiple regulatory environments. Smaller companies especially need affordable technology solutions to remain competitive while supporting user trust.
In the future, successful companies will be those that foster fair data relationships, where users understand the value exchange and feel like partners rather than "products".

7.4 Regulatory aspects and challenges in shaping forward-looking guidelines

This section addresses P4: Legal compliance mechanisms increase the credibility of personalization strategies in the eyes of customers and clients.
Legislators must account for varying levels of digital maturity among organizations and support less developed companies in building compliant and ethical infrastructures. Clear regulations, standard-setting, and incentives for adopting PETs can reduce uncertainty and encourage innovation. Regulations must also remain adaptable, as AI and personalization technologies evolve rapidly. Static regulations risk creating legal gaps or inconsistent enforcement.
Collaboration between industry, academia, and civil society is essential to developing practical governance mechanisms.
Future legislation should also promote data citizenship, empowering individuals with rights and responsibilities regarding how their data is collected, shared, and used (Hanegan, 2023).

Principles of transparency, control, and reciprocity should be further embedded both in regulation and in the design of technology platforms, contributing to fairer and more trustworthy digital marketing.

7.5 The dangers of using first-party data with AI and developing an ethical infrastructure of the future

Artificial intelligence processing first-party data is not just a targeting tool since it is becoming an active designer of the information environment.
AI-driven recommender systems can create filter bubbles, where users are exposed only to content that reinforces their existing beliefs, leading to social polarization. AI systems optimizing attention (clicks, purchases, engagement) can exploit emotions, habits, and vulnerabilities, leading to manipulative practices.
Historical examples, such as Cambridge Analytica, highlight the dangers of algorithmic manipulation of public opinion. Thus, the future will not only be about who controls the data, but also about who controls the algorithms that process our data and whether these algorithms serve the public good.
Regulators must set clear guidelines and prove an ethical infrastructure for AI management of first-party data, like what GDPR achieved for data privacy.

This ought to include:

1. algorithmic transparency (how do they make decisions?);
2. data charters (what companies collect, how they use it and who they share it with);
3. digital trust contracts (what users can expect in return for their data);

4. independent oversight mechanisms to monitor the use of data and algorithms (like the Information Privacy Commissioner responsible for compliance with GDPR).

8 CONCLUSION

This study has examined the relationship between first-party data strategies, artificial intelligence (AI)-driven personalization, and consumer trust, offering an integrated framework for aligning personalization practices with ethical and regulatory standards. Combining empirical findings from iPROM's (2025) research with existing academic and practitioner literature, the paper demonstrates that effective data governance is central to ethical personalization in AI-based marketing.

The analysis shows that companies with higher data governance maturity (48.1% of Slovenian firms in the sample) implement systematic privacy practices, including regular audits, the use of privacy-enhancing technologies (PETs), and compliance checks. These companies are demonstrably more likely to conduct AI-driven personalization that aligns with principles of transparency, fairness, and legal compliance. In contrast, organizations with low data maturity (17%) rely on ad hoc data practices, which correlate with lower levels of perceived ethicality and trust in their personalization efforts.

Furthermore, 75.4% of surveyed companies recognize first-party data as a strategic asset (iPROM, 2025), confirming the growing importance of data governance in achieving both marketing effectiveness and regulatory compliance. Organizations that operationalize data transparency, informed consent, and user empowerment in their data strategies can strengthen trust and enhance customer relationships, while also reducing reputational and legal risks.

The framework developed in this study highlights that the integration of PETs, dynamic consent models, and transparent data governance mechanisms directly contributes to more ethical and effective personalization outcomes. Moreover, consumers increasingly expect active participation in data exchanges, consistent with emerging models of data citizenship and fair value exchange (Quach et al., 2022; Martin & Palmatier, 2019). Organizations that meet these expectations are better positioned to foster long-term loyalty and engagement.

In the contemporary data economy, trust functions as a measurable business asset. The ability to manage first-party data in a transparent and ethically sound manner has become a key differentiator in the marketplace. Companies that embed these principles into their AI personalization strategies are more likely to achieve sustainable competitive advantages and build enduring relationships with consumers.

This paper contributes to the growing discourse on corporate digital accountability and data citizenship. However, given that the empirical evidence is based on a modest and non-representative sample of Slovenian companies (iPROM, 2025), future research should expand to larger, cross-national samples and adopt longitudinal designs to confirm and further refine the proposed framework.

References

Alwabel, R. A., & Fatunmbi, T. O. (2024). Personalized marketing strategies leveraging data science to tailor marketing campaigns based on customer data. World Journal of Advanced Research and Reviews, 13(1), 832–846. https://www.researchgate.net/publication/385379779_Personalized_Marketing_Strategies_Leveraging_Data_Science_to_Tailor_Marketing_Campaigns_Based_on_Customer_Data

Chen, H., Ren, X., He, L., & Huang, J. (2024, October). Editorial: AI as intelligent technology and agent to understand and be understood by human minds. Frontiers in Psychology. https://doi.org/10.3389/fpsyg.2024.1461881

Da Bormida, M. (2022). The big data world: Benefits, threats and ethical challenges. In D. Wright & M. Friedewald (Eds.), Ethical issues in covert, security and surveillance research (Vol. 8, pp. 71–91). Emerald Publishing. https://doi.org/10.1108/S2398-601820210000008007

Elly, B. (2025). Ethical implications of data collection in personalized marketing. ResearchGate. https://www.researchgate.net/publication/388514697_Ethical_Implications_of_Data_Collection_in_Personalized_Marketing

EY. (2023). Six steps to confidently manage data privacy in the age of AI. Ernst & Young Global. https://www.ey.com/en_pl/insights/law/six-steps-to-confidently-manage-data-privacy-in-the-age-of-ai

Davenport, T. H., Guha, A., Grewal, D., & Bressgott, T. (2020). How artificial intelligence will change the future of marketing. Journal of the Academy of Marketing Science, 48(1), 24–42. https://link.springer.com/content/pdf/10.1007/s11747-019-00696-0.pdf

Gao, B., Wang, Y., Xie, H., & Hu, Y. (2023). Artificial intelligence in advertising: Advancements, challenges, and ethical considerations in targeting, personalization, content creation, and ad optimization. SAGE Open, 13(4), 1–20. https://doi.org/10.1177/21582440231210759

Google, IPSOS. (2020). Privacy by design: exceeding customer expectations. https://www.thinkwithgoogle.com/_qs/documents/12053/Google_Privacy_Report_ebook_FA_1.pdf

Hanegan, K. (2023, July 26). Embracing data citizenship: Empowering individuals in the age of algorithmic decision-making. Turning Data Into Wisdom. https://www.turningdataintowisdom.com/embracing-data-citizenship/

iPROM. (2025). Protection of companies' proprietary data and the transition to first-party data strategies in digital advertising. iPROM Labs, Research Report. https://iprom.si/blog/ipromova-raziskava-zascita-lastnih-podatkov-in-pomen-za-ucnkovitost-oglasevalskih-strategij/

iPROM. (2025). Real-time creative. https://iprom.si/produkti/iprom-real-time-creative/

Kennedy, H., Ditchfield, H., Oman, S., & Bates, J. (2024). How people connect fairness and equity when they talk about data uses. Big Data & Society. https://doi.org/10.1177/20539517241303162

Martin, K. D. & Palmatier, R. W., (2019). The ethicality of customer data monetization: Issues and frameworks. Journal of Business Research, 100, 254–263. https://www.researchgate.net/publication/305822708_Data_Privacy_Effects_on_Customer_and_Firm_Performance

Martin, K. D., & Palmatier, R. W. (2020). Data privacy in retail. Journal of Retailing, 96(4), 474–489. https://pmc.ncbi.nlm.nih.gov/articles/PMC7505556/

Nwobodo, L. K. (2025). The impacts of big data analytics and artificial intelligence on marketing. Global Journal of Economics and Financial Research. https://www.researchgate.net/publication/388089017_The_Impacts_of_Big_Data_Analytics_and_Artificial_Intelligence_on_Marketing_Strategies

OECD. (2023). Emerging Privacy-Enhancing Technologies: Current Regulatory & Policy Approaches. OECD Digital Economy Papers, No. 3512. Published March 2023.

Perko, I. (2023). Data sharing concepts: A viable system model diagnosis. Kybernetes, 52(9), 2976–2991. https://doi.org/10.1108/K-04-2022-0575

Romansky, R. P., & Noninska, I. (2020). Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering, 17(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Quach, S., Thaichon, P., Martin, K. D., Iaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Shopify. (2024). First-party data and privacy-centric marketing. Shopify White Paper. https://www.shopify.com/enterprise/blog/first-party-data

Singla, K., Rana, M., & Bansal, J. (2023, November). The future of OpenAI tools: Opportunities and challenges for human-AI collaboration. In Proceedings of the 2023 2nd International Conference on Futuristic Technologies (INCOFT) (pp. 1–6). IEEE. https://doi.org/10.1109/INCOFT60753.2023.10424990

World Economic Forum. (2025). Digital trust decision-making for trustworthy technology. https://initiatives.weforum.org/digital-trust/home

Xu, T., Shi, H., Shi, Y., & You, J. (2024). From data to data asset: Conceptual evolution and strategic imperatives in the digital economy era. Asia Pacific Journal of Innovation and Entrepreneurship, 18(1), 2–20. https://doi.org/10.1108/APJIE-10-2023-0195

Yadav, T. C., Roy Kolachina, R. I., & Kanneganti, M. C. (2024). Data Privacy Concerns and their Impact on Consumer Trust in Digital Marketing. International Journal of Scientific Research in Engineering and Management, 08(11), 1–7. https://www.researchgate.net/publication/305822708_Data_Privacy_Effects_on_Customer_and_Firm_Performance