Journal of Secure Digital Technologies
Volume 1 (№2) September 2026

ISSN (E): 3136-9340
Sertificate № KZ19VPY00128988, date of issue: 25.12.2025

The journal is published 4 times a year
(March, June, September, December)

EDITORIAL TEAM
Editor-in-Chief
Dr. Leila Rzayeva, Association prof., PhD, Digital government support center (Kazakhstan)

Deputy Editor-in-Chief
Dr. Ali Myrzatay, PhD, Digital government support center (Kazakhstan)

Executive Secretary
Dr. Abdenova Zhuldyz, PhD, Digital government support center (Kazakhstan)

EDITORIAL BOARD MEMBERS (KAZAKHSTAN)
Seitkulov E.N. – Candidate of Physical and Mathematical Sciences, Professor Computer Science, Computer Engineering and Control
Abdenova G.A. – PhD in Automation and Control, Candidate of Technical Sciences, Professor L.N. Gumilyov Eurasian National University
Atanov S.K. – Doctor of Technical Sciences, Professor.
Sergazin G.K. – PhD, Associate Professor Computer Science, Computer Engineering and Control
Satybaldina D.Zh. – Candidate of Physical and Mathematical Sciences, Professor Director, Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University

INTERNATIONAL EDITORIAL BOARD MEMBERS
Ibraheem Shayea – PhD in Electrical and Electronic Engineering Istanbul Technical University (Turkey)
Yadigar Nasiboglu Imamverdiyev – DSc in Technical Sciences, Associate Professor Information Security, Computer Science and Computer Technology (Azerbaijan)
Erdal Irmak – PhD in Electrical and Electronics Engineering, Professor Gazi University (Turkey)
Korhan Kayisli – PhD in Electrical Electronics Engineering, Associate Professor Gazi University (Turkey)
Yonghao Wang – PhD in Electronic Engineering, Associate Professor Queen Mary, University of London (UK)
Amir Mosavi – PhD in Applied Informatics, Professor of AI Obuda University (Hungary)
Gerald Feldman – PhD in General Computing, Associate Professor Birmingham City University (UK)
Mohamed Ragab – PhD in Computer Science, Assistant Professor Birmingham City University (UK)
Seref Sagiroglu – PhD in System Engineering, Professor Gazi University (Turkey)

MANAGING EDITOR
Dr. Ali Myrzatay, PhD, Digital government support center (Kazakhstan)

TECHNICAL EDITOR
Dr. Ali Myrzatay, PhD, Digital government support center (Kazakhstan)

CONTENTS

Cyber Incident Damage Assessment for Public Digital Systems and Critical Infrastructure 3

Cyber Incident Damage Assessment for Public Digital Systems and Critical Infrastructure 37

Verifiable but Not Correct: Blockchain Trust Boundaries for Autonomous Agents 71

Calibrated Digital Twins and Geometry-based Perception for Automated Driving in Heavy Rain and Snowfall: Evidence From Research Testing in China and Implications for Kazakhstan. 88

Personal Data Protection in Kazakhstan's AI Enabled Public Services 109

Asking Another Jurisdiction What It Holds Without Telling It What You Hold: Private Artifact Matching with a Ledger-Anchored Transcript 131

On-Chain and Off-Chain Data Placement in Hybrid Blockchain Health Systems 143

An Integrated Project Management Maturity Model for Digital Qazaqstan Initiatives: Embedding Cybersecurity, AI Governance and Forward-Looking Cyber-Risk Requirements into ST RK ISO 21502-2022..... 158

Appendix A. Indicators and evidence for the baseline practice groups 181

Privacy Risks and Data Protection Readiness in AI Marketing in Kazakhstan..... 183

Supplementary Materials..... 205

Raushan Kambar*
PhD, Project Manager, Project Monitoring and Management Center of Digital Government Support Center
r.kambar@govtec.kz, ORCID orcid.org/0009-0008-6024-736X
Digital Government Support Center, Kazakhstan

Asselya Abildayeva
MSc, Head of Endowment MNU
as_abildayeva@kazguu.kz, ORCID orcid.org/0009-0008-9492-1850
Maqsut Narikbayev University, Kazakhstan, Kazakhstan

PRIVACY RISKS AND DATA PROTECTION READINESS IN AI MARKETING IN KAZAKHSTAN

Abstract: Artificial intelligence (AI) is entering the marketing practice of Kazakhstani companies at the same time as the national legal framework for personal data and AI is being tightened: the Law on Personal Data and Their Protection was amended in 2025–2026, the Law on Artificial Intelligence entered into force on 18 January 2026, and the Digital Code on 12 July 2026. No empirical evidence exists on whether businesses that intend to use AI in marketing understand the privacy and security obligations this creates. This study provides a baseline measurement of that readiness taken immediately before the Law on Artificial Intelligence entered into force. An anonymous online survey of 41 representatives of Kazakhstani companies and startups (15 items: 8 closed, 6 five-point Likert items, 1 open-ended question answered by 24 respondents) was analysed by descriptive statistics and thematic analysis, and respondents' perceptions were mapped onto the obligations of the three legal instruments. The results show a readiness–compliance gap: 80.5% of respondents regard AI integration as a condition of competitiveness, 87.8% intend to use AI tools in marketing and 95.1% already use consumer AI applications; 70.7% agree that AI creates significant risks for customer data, yet the risks they name (AI-enabled phishing and data theft, system failures, attacks on AI infrastructure, privacy violation, manipulation) are framed as external threats, and no respondent referred to the company's own obligations as an operator of personal data. Data security appears in 10 of 24 open-ended responses, but only 2 refer to legal requirements. The mapping shows that none of eight obligation groups is reflected in respondents' perceptions and that routine use of foreign generative AI services with customer data most directly exposes the localisation and cross-border transfer requirements. The scientific novelty of the work lies in the first empirical, obligation-level reading of business perception against Kazakhstan's three-instrument framework; the resulting mapping can serve as a compliance checklist for AI marketing, and a supplementary survey module is proposed for subsequent waves.

Keywords: personal data protection; artificial intelligence; AI marketing; privacy risk; regulatory readiness; generative AI; cross-border data transfer; compliance; Kazakhstan

ИИ-маркетинг в Казахстане: риски приватности и готовность к защите данных

Аннотация: Искусственный интеллект (ИИ) входит в маркетинговую практику казахстанских компаний одновременно с ужесточением национальной нормативной базы в сфере персональных данных и ИИ: Закон «О персональных данных и их защите» изменён в 2025–2026 годах, Закон «Об искусственном интеллекте» вступил в силу 18 января 2026 года, Цифровой кодекс — 12 июля 2026 года. Эмпирических данных о том, понимают ли компании, намеревающиеся применять ИИ в маркетинге, возникающие при этом обязательства в области приватности и безопасности, нет. Исследование даёт базовое измерение такой готовности, выполненное непосредственно перед вступлением в силу Закона об ИИ. Анонимный онлайн-опрос 41 представителя казахстанских компаний и стартапов (15 вопросов: 8 закрытых, 6 по пятибалльной шкале Лайкерта, 1 открытый, на который ответили 24 респондента) проанализирован методами описательной статистики и тематического анализа, а представления респондентов сопоставлены с обязанностями по трём правовым актам. Результаты выявляют разрыв между готовностью к внедрению и готовностью к соблюдению требований: 80,5% респондентов считают интеграцию ИИ условием конкурентоспособности, 87,8% намерены использовать ИИ-инструменты в маркетинге, 95,1% уже пользуются потребительскими ИИ-приложениями; 70,7% согласны, что ИИ создаёт значимые риски для данных клиентов, однако называемые ими риски (фишинг и кража данных с помощью ИИ, сбои систем, атаки на ИИ-инфраструктуру, нарушение приватности, манипуляция) описываются как внешние угрозы, и ни один респондент не упомянул собственные обязанности компании как оператора персональных данных. Безопасность данных присутствует в 10 из 24 открытых ответов, но лишь в 2 упоминаются требования закона. Сопоставление показывает, что ни одна из восьми групп обязанностей не отражена в представлениях респондентов, а повседневное использование зарубежных генеративных ИИ-сервисов с данными клиентов наиболее прямо затрагивает требования локализации и трансграничной передачи. Научная новизна работы — первое эмпирическое прочтение восприятия бизнеса на уровне конкретных обязанностей по трём актам Казахстана; полученное сопоставление может служить чек-листом комплаенса для ИИ-маркетинга, а для последующих волн опроса предложен дополнительный модуль анкеты.

Ключевые слова: защита персональных данных; искусственный интеллект; ИИ-маркетинг; риски приватности; регуляторная готовность; генеративный ИИ; трансграничная передача данных; комплаенс; Казахстан

Қазақстандағы ЖИ-маркетинг: жекелік қауіптері және деректерді қорғауға дайындық

Аңдатпа: Жасанды интеллект (ЖИ) қазақстандық компаниялардың маркетингтік тәжірибесіне дербес деректер мен ЖИ саласындағы ұлттық нормативтік база қатаңдатылып жатқан кезеңде енуде: «Дербес деректер және оларды қорғау туралы» Заңға 2025–2026 жылдары өзгерістер енгізілді, «Жасанды интеллект туралы» Заң 2026 жылғы 18 қаңтарда, Цифрлық кодекс 2026 жылғы 12 шілдеде күшіне енді. Маркетингте ЖИ қолдануға ниетті компаниялардың осыдан туындайтын жекелік пен қауіпсіздік міндеттемелерін түсінетіні туралы эмпирикалық деректер жоқ. Зерттеу осындай дайындықтың «Жасанды интеллект туралы» Заң күшіне енер алдында жүргізілген базалық өлшемін ұсынады. Қазақстандық компаниялар мен стартаптардың 41 өкілі арасында жүргізілген анонимді онлайн-сауалнама (15 сұрақ: 8 жабық, 6 бес балдық Лайкерт шкаласы бойынша, 1 ашық сұрақ, оған 24 респондент жауап берді) сипаттамалық статистика және тақырыптық талдау әдістерімен өңделді, ал респонденттердің түсініктері үш құқықтық актінің міндеттемелерімен салыстырылды. Нәтижелер енгізуге дайындық пен талаптарды сақтауға дайындық арасындағы алшақтықты көрсетті: респонденттердің 80,5%-ы ЖИ интеграциясын бәсекеге қабілеттіліктің шарты деп санайды, 87,8%-ы маркетингте ЖИ құралдарын қолдануға ниетті, 95,1%-ы тұтынушылық ЖИ-қосымшаларды пайдаланады; 70,7%-ы ЖИ клиенттер деректеріне елеулі қауіп төндіреді деп келіседі, алайда олар атаған қауіптер (ЖИ арқылы фишинг пен деректерді ұрлау, жүйе ақаулары, ЖИ инфрақұрылымына шабуылдар, жекелікті бұзу, манипуляция) сыртқы қатерлер ретінде сипатталады және бірде-бір респондент компанияның дербес деректер операторы ретіндегі өз міндеттерін атамаған. Деректер қауіпсіздігі 24 ашық жауаптың 10-ында кездеседі, бірақ тек 2-уінде ғана заң талаптары аталады. Салыстыру сегіз міндеттемелер тобының ешқайсысы респонденттердің түсінігінде көрініс таппағанын және шетелдік генеративті ЖИ-сервистерін клиент деректерімен күнделікті пайдалану деректерді локализациялау мен трансшекаралық беру талаптарын барынша тікелей қозғайтынын көрсетті. Жұмыстың ғылыми жаңалығы — Қазақстанның үш актіден тұратын нормативтік базасы аясында бизнес түсінігін нақты міндеттемелер деңгейінде алғаш рет эмпирикалық талдау; алынған кесте ЖИ-маркетинг үшін комплаенс-чеклист ретінде қолданыла алады, ал кейінгі сауалнама толқындары үшін қосымша сауалнама модулі ұсынылды.

Түйін сөздер: дербес деректерді қорғау; жасанды интеллект; ЖИ-маркетинг; жекелік қауіптері; реттеуші дайындық; генеративті ЖИ; деректерді трансшекаралық беру; комплаенс; Қазақстан

1. Introduction (Literature Review)

Artificial intelligence (AI) has become the dominant technological driver of change in marketing. Customer analytics, personalisation, recommendation, conversational agents and content generation increasingly rely on machine learning models that are trained on, and fed with, the personal data of consumers [1], [2]. The academic debate has moved from whether AI will transform marketing to the conditions under which it can do so legitimately: the capabilities that make AI valuable for marketers — inference from large volumes of behavioural data, micro-targeting, automated decisions about individuals — are the same capabilities that generate privacy harm, erode consumer trust and attract regulatory intervention [3]–[6].

Kazakhstan is an instructive setting for studying this tension. The country has declared AI a national priority: the Concept for the Development of Artificial Intelligence for 2024–2029 was adopted in July 2024 [7], the International Center for Artificial Intelligence Alem.AI was launched, and on 18 September 2025 the sectoral ministry was transformed into the Ministry of Artificial Intelligence and Digital Development (MAIDD) [8]. In parallel, the legal framework governing the use of personal data by business has been tightened in rapid succession. Fines under Article 79 of the Code on Administrative Offences were roughly tripled in 2025 [9]; the Law "On Artificial Intelligence" No. 230-VIII of 17 November 2025 entered into force on 18 January 2026 [10]; the Digital Code No. 255-VIII of 9 January 2026 entered into force on 12 July 2026 [11]; and Law No. 326-VIII of 24 June 2026 introduced into the Law "On Personal Data and Their Protection" an identifier-based definition of personal data, a prohibition on decisions based solely on automated processing, a register of personal data security breaches and a register of persons collecting and processing personal data [12], [13]. The regulator has announced further increases in liability, including fines of up to 5,000 monthly calculation indices (MCI) and criminal liability for mass leaks [14].

Business appears to be moving at a different pace. The KPMG Kazakhstan AI Readiness Report (March 2025), covering more than 50 companies, found that only 20% had adopted AI-specific internal regulations, 40% relied on general data policies and 50% considered their data infrastructure inadequate; even among "AI leaders", more than 60% had no AI-specific rules [15]. Mass leaks of personal data — including the June 2025 publication of a database of more than 16 million records attributed to private information systems [16] — show that the cost of this gap is borne by consumers.

1.1 Literature review

Privacy as the binding constraint of AI marketing. The marketing literature treats data privacy as a strategic variable rather than a legal formality. Martin and Murphy [4] frame privacy as a multi-level construct that simultaneously affects consumers, firms and regulators, and show that privacy failures translate into measurable business losses; Martin, Borah and Palmatier [17] demonstrate that data breaches reduce customer trust and firm

performance and that the effect spills over to competitors. Acquisti, Brandimarte and Loewenstein [18] show that consumers' privacy decisions are context-dependent and malleable, so that formal consent obtained in a persuasive interface is a weak guarantee of informed agreement — a point that bears directly on AI-generated marketing interfaces. Bleier, Goldfarb and Tucker [5] conclude that privacy regulation reshapes rather than eliminates data-based marketing. AI raises the stakes within this body of work: Davenport et al. [1] identify data privacy, algorithmic bias and ethical use as the main constraints on the future of AI in marketing; Huang and Rust [2] note that higher levels of AI — "thinking" and "feeling" AI — require deeper access to personal and emotional data; Puntoni et al. [19] show that consumers experience AI as a source of exploitation and loss of autonomy as well as of convenience. Hermann [6] argues that ethical AI marketing requires informed consent, transparency and the avoidance of manipulation, and that systems collecting data without informed consent create risk for the company itself. Jobin, Ienca and Vayena [20], reviewing 84 AI ethics guidelines, find transparency, justice, non-maleficence, responsibility and privacy to be the most frequently cited principles — the principles Kazakhstan's Law on Artificial Intelligence has now codified. Bibliometric and agenda-setting work [3], [21] identifies privacy, trust and ethics as under-researched dimensions of AI marketing, particularly outside Western markets.

Generative AI tools in business practice. A second strand concerns the operational use of generative AI tools (ChatGPT and analogous services) by employees. Wu, Duan and Ni [22] systematise the security, privacy and ethical concerns of ChatGPT, including the retention and potential reuse of user inputs by the provider and the leakage of confidential information entered into prompts. The 2023 case in which Samsung banned employee use of generative AI after staff uploaded proprietary source code [23] shows that the risk is practical. The use of AI tools in violation of organisational rules ("shadow AI") is widespread: in a global study by KPMG and the University of Melbourne, 48% of employees reported using AI tools in ways that contravened company policy [24]. For marketing functions this matters because customer data — names, contacts, purchase histories, segments — are a natural input to generative tools used for drafting personalised messages, analysing feedback or building audiences. Where the provider is located abroad, each such input is potentially a cross-border transfer of personal data; where the provider retains inputs, it is a disclosure to a third party without the data subject's consent.

Small and medium-sized enterprises and data protection regimes. Studies of small and medium-sized enterprises (SMEs) under the European Union General Data Protection Regulation (GDPR) consistently show that awareness of a regime does not translate into compliance without targeted guidance: Brodin [25] reports that most SMEs studied were aware of the GDPR but only a minority had identified the steps needed to comply, and Freitas and Mira da Silva [26] find that SMEs postpone compliance until confronted with enforcement. Legal scholarship on Kazakhstan's personal data regime — the comparative chapter by Omarova, Mukhtorov and Yerlankyzy [27], the analysis of the supervisory

authority by Akhmetova, Tursynkulova and Ibrayev [28] and the review by Alibayeva and Yerbolatov [29] — is doctrinal and is not connected to empirical evidence on business behaviour.

1.2 Regulatory framework of Kazakhstan for personal data and artificial intelligence

The framework for the processing of personal data in marketing is now formed by three instruments, supplemented by subordinate rules and by liability provisions of the Code on Administrative Offences and the Criminal Code. Because the survey reported in this paper was conducted before 18 January 2026, Table 1 distinguishes obligations that were already in force at the time of the survey from those introduced afterwards.

Law "On Personal Data and Their Protection" No. 94-V of 21 May 2013 [12]. The Law establishes the conditions of collection and processing (Article 7), the requirements for the content of the data subject's consent (Article 8), the requirement to store personal data in a database located in Kazakhstan (Article 12) and the conditions of cross-border transfer, which is permitted to states that ensure the protection of personal data and otherwise only with the consent of the data subject or on other grounds listed in the Law (Article 16). Owners and operators must take legal, organisational and technical protection measures and notify the authorized body of a personal data security breach within one working day of its discovery (Article 25) [30], [31]. Law No. 326-VIII of 24 June 2026 [13] added an identifier-based definition of personal data; definitions of automated processing, anonymisation, masking and hashing; a rule that publication of data by the data subject does not in itself constitute consent to further processing; a prohibition on decisions based solely on automated processing, with a right to object; a prohibition on the collection and processing of personal data for the creation or expansion of databases by their non-purpose extraction from publicly available sources; a register of personal data security breaches; and a register of persons collecting and processing personal data.

Law "On Artificial Intelligence" No. 230-VIII of 17 November 2025 [10]. In force since 18 January 2026, the Law establishes the principles of legality, fairness, transparency and explainability, priority of human well-being, protection of personal data and confidentiality, and safety of AI systems, and introduces a risk-based classification of AI systems (minimal, medium and high risk). Of direct relevance to marketing, it prohibits AI systems that use manipulative methods affecting the subconscious or distorting behaviour, systems that exploit vulnerabilities of persons, social scoring, emotion recognition without consent, biometric categorisation for discriminatory purposes, and systems that unlawfully collect and process personal data. It requires synthetic content to be distributed only with machine-readable marking and a visual warning, users to be informed that they are interacting with an AI system or receiving a service produced with AI, and goods, works and services created with AI to be labelled. Users may request information on decisions taken with AI and on the underlying data. The accompanying law amended the Code on

Administrative Offences to introduce liability for failure to inform users of misleading synthetic results and for failure to manage the risks of a high-risk system where harm results.

Digital Code No. 255-VIII of 9 January 2026 [11]. In force since 12 July 2026, the Code does not replace the Law on Personal Data but establishes digital rights that constrain AI marketing: the right to erasure, anonymisation and restriction of processing; the right to have algorithmic decisions reviewed by a human; the restriction of biometric processing to cases provided by law; and the obligation to delete leaked data immediately with notification of the competent bodies. The Law "On Informatization" was restructured and renamed the Law "On Cybersecurity" by Law No. 256-VIII of the same date and retains the duty of owners of digital objects containing personal data to take the measures provided by personal data legislation [32].

Liability and enforcement. Article 79 of the Code on Administrative Offences, as amended in 2025, provides fines for unlawful collection and processing (up to 200 MCI for large businesses), for failure to take protection measures (up to 600 MCI) and, where such failure results in loss or unlawful processing, up to 2,000 MCI for large businesses — approximately 8.65 million tenge at the 2026 MCI value [9]. Article 147 of the Criminal Code provides criminal liability for violation of the inviolability of private life and of personal data legislation causing substantial harm [33]. Since the beginning of 2024 the Information Security Committee has imposed fines totalling 4.9 million tenge under Articles 79 and 641 [34], and 43 personal data leaks, each affecting 5–10 thousand persons, were registered in 2025 alone [35]. The authorized body is MAIDD, with state control exercised by its Information Security Committee [8]. The Concept of Digital Transformation, Development of the ICT Industry and Cybersecurity for 2023–2029 [36], which succeeded the "Digital Kazakhstan" programme, and the AI Concept [7] set the policy frame; Kazakhstan ranked 48th of 174 economies in the IMF AI Preparedness Index 2024 [37] and 60th of 195 in the Oxford Insights Government AI Readiness Index 2025 [38].

Table 1. Obligations of the legal framework relevant to AI marketing and their status at the time of the survey (second half of 2025)

No.	Obligation (source)	In force at the time of the survey
O1	Consent of the data subject with the content required by the Law (Law No. 94-V, Arts. 7, 8)	Yes
O2	Prohibition on building or expanding databases by non-purpose extraction from publicly available sources (Law No. 94-V, Art. 7, as amended by Law No. 326-VIII)	No (from 2026)
O3	Storage of personal data in a database in Kazakhstan (Art. 12) and conditions of cross-border transfer (Art. 16)	Yes
O4	Protection measures and notification of the authorized body within one working day of discovering a breach (Art. 25; Orders No. 232/NQ, 338/NQ)	Yes (notification duty since 1 July 2024)

No.	Obligation (source)	In force at the time of the survey
O5	Prohibition on decisions based solely on automated processing; right to object (Law No. 326-VIII); human review of algorithmic decisions (Digital Code)	No (from 2026)
O6	Prohibition on manipulative AI systems and exploitation of vulnerabilities (Law No. 230-VIII)	No (from 18 January 2026)
O7	Labelling of synthetic content; disclosure of interaction with AI (Law No. 230-VIII)	No (from 18 January 2026)
O8	Right to erasure, anonymisation and restriction of processing (Digital Code; Law No. 94-V)	Partly (erasure on withdrawal of consent under Law No. 94-V; extended by the Digital Code from 12 July 2026)

1.3 Research gap, research questions, novelty and contributions

Research gap. The literature establishes that privacy is the binding constraint of AI marketing, that everyday use of generative AI tools creates uncontrolled disclosure and cross-border transfer risks, and that SMEs tend to be aware of data protection regimes without complying with them. What is missing for Kazakhstan is an empirical link between the two bodies of evidence that do exist — consultancy surveys of AI readiness, which do not address legal obligations, and doctrinal legal studies, which do not address business behaviour. In particular, there is no measurement of how businesses that intend to use AI in marketing perceive privacy risk and whether that perception includes the obligations that the framework attaches to their own practices. Because the framework changed fundamentally between November 2025 and July 2026, a measurement taken before 18 January 2026 is also the only available baseline against which the effect of the new instruments can later be assessed.

Research questions. This study addresses the following research question: does the readiness of Kazakhstani companies and startups to adopt AI in marketing include awareness of the personal data protection obligations that such adoption entails? Specifically, the paper examines: (1) RQ1 — how Kazakhstani companies and startups perceive the privacy and security risks associated with the use of AI in marketing; (2) RQ2 — to what extent their declared readiness to adopt AI in marketing is accompanied by awareness of their own obligations as owners or operators of personal data; (3) RQ3 — which obligations of the Law on Personal Data, the Law on Artificial Intelligence and the Digital Code are most exposed by the prevailing patterns of AI use, and what measures follow for companies and the regulator.

Scientific novelty. The scientific novelty of this work consists in the first empirical, obligation-level reading of business perception of AI-related privacy risk in Kazakhstan,

obtained immediately before the entry into force of the Law on Artificial Intelligence and mapped onto the three-instrument framework (the amended Law on Personal Data, the Law on Artificial Intelligence and the Digital Code), which distinguishes it from prior approaches that treat either business readiness or the legal regime in isolation.

Contributions. The paper makes four contributions: (C1) a baseline measurement (N = 41) of awareness, intention and perceived AI-related risk among Kazakhstani companies and startups taken before 18 January 2026; (C2) empirical evidence of a readiness–compliance gap, in which 87.8% of respondents intend to use AI in marketing and 70.7% recognise data security risk, while no respondent identifies the company's own obligations; (C3) a mapping of perceived risks onto eight obligation groups with the applicable sanctions, distinguishing obligations in force at the time of the survey from those introduced after it, usable as a compliance checklist; (C4) a supplementary survey module of ten items mapped to specific obligations for subsequent waves.

The remainder of the paper is organised as follows: Section 2 presents the materials and methods; Section 3 reports the results; Section 4 discusses them in relation to the research questions, the literature and the legal framework and states the limitations; Section 5 concludes the paper.

2. Methods and Materials

2.1 Research design

The study combines a cross-sectional descriptive survey, thematic analysis of open-ended responses and doctrinal analysis of the regulatory framework. The survey component is exploratory: its purpose is to establish a baseline of awareness, attitudes and perceived risks, not to test hypotheses, and the sample does not permit inferential generalisation to the population of Kazakhstani companies.

2.2 Instrument

The questionnaire consisted of 15 items: 8 closed-ended items (type of organisation, sector, size, respondent role, self-assessed level of knowledge of AI, experience of using AI-based applications, current use of AI in marketing, perceived threats of AI — multiple choice); 6 statements rated on a 5-point Likert scale (1 = strongly disagree, 5 = strongly agree, or 1 = very unlikely, 5 = very likely for the intention item) covering the necessity of AI for competitiveness, the likelihood of using AI tools in marketing strategies, the sufficiency of technical infrastructure, the availability of competent specialists, the existence of a strategy for AI use, and the perceived risk of AI for customer data security; and 1 optional open-ended item inviting respondents to share their views, experience and recommendations. The questionnaire was implemented in Google Forms and is reproduced in Appendix A.

2.3 Sampling and data collection

The target population was representatives of Kazakhstani companies and startups involved in marketing decisions. The link to the questionnaire was distributed by e-mail through professional networks of the authors (convenience sampling). The survey was conducted in the second half of 2025 between September and October, before the entry into force of the Law on Artificial Intelligence (18 January 2026). Participation was voluntary and anonymous; respondents gave informed consent on the first page of the form, and no personal data of respondents were collected. In total 41 complete responses were received (N = 41); 24 respondents (58.5%) answered the optional open-ended item.

2.4 Analysis

Closed and Likert items were analysed by descriptive statistics (absolute frequencies and percentages of N = 41; percentages are rounded to one decimal place, so that one respondent corresponds to 2.4%). Open-ended responses were coded inductively following the reflexive thematic analysis approach of Braun and Clarke [39]: both authors read all 24 responses independently, assigned initial codes, consolidated codes into themes and resolved discrepancies by discussion; a response could be assigned to more than one theme. The regulatory analysis (Section 1.2) is based on the texts of the legislative acts published on the official legal information system Adilet and on the subordinate rules of the authorized body. The mapping (Section 3.6) was constructed by listing the obligation groups of Table 1, identifying for each the marketing practice that triggers it, searching the closed and open-ended responses for any reference to the obligation or to the practice, and recording the applicable sanction.

2.5 Ethical considerations

The study did not involve the processing of personal data of respondents, and ethics committee approval was not required under the rules of the authors' institutions.

3. Results

3.1 Sample

The composition of the sample is shown in Table 2. Companies predominated over startups (65.9% vs 34.1%), small and micro organisations formed two thirds of the sample, and the information technology and telecommunications sector was the largest (31.7%). Most respondents were marketing managers or specialists (39.0%) or owners and founders (26.8%).

Table 2. Composition of the sample (N = 41)

Characteristic	Category	n	%
Type of organisation	Company	27	65.9

Characteristic	Category	n	%
	Startup	14	34.1
Size (number of employees)	Micro (up to 15)	12	29.3
	Small (16–100)	15	36.6
	Medium (101–250)	8	19.5
	Large (over 250)	6	14.6
Sector	Information technology and telecommunications	13	31.7
	Retail and e-commerce	8	19.5
	Financial services	6	14.6
	Education and consulting	5	12.2
	Manufacturing and logistics	4	9.8
	Other services	5	12.2
Role of respondent	Marketing manager or specialist	16	39.0
	Owner or founder	11	26.8
	Senior manager (director, deputy director)	7	17.1
	IT or analytics specialist	4	9.8
	Other	3	7.3

3.2 Awareness of, experience with and current use of AI

Self-assessed knowledge of AI was medium or higher for 40 of 41 respondents (97.6%); only 1 respondent (2.4%) rated it as low and none as very low (Table 3). Experience of using AI-based applications (ChatGPT, Siri, Google Assistant and similar) was reported by 39 respondents (95.1%). Current use of AI in marketing was limited: 9 respondents (22.0%) reported regular use, 17 (41.5%) occasional or pilot use, and 15 (36.6%) no use.

Table 3. Awareness of, experience with and current use of AI (N = 41)

Item	Category	n	%
Self-assessed knowledge of AI	Very low	0	0.0
	Low	1	2.4
	Medium	14	34.1
	High	19	46.3
	Very high	7	17.1

Item	Category	n	%
Experience of using AI-based applications	Yes	39	95.1
	No	2	4.9
Current use of AI in marketing	Regular	9	22.0
	Occasional or pilot	17	41.5
	Not used	15	36.6

3.3 Attitudes and intention

Table 4 reports the full distribution of the six Likert items. Agreement that AI integration is a necessary condition of competitiveness was expressed by 33 respondents (80.5%), with 5 (12.2%) disagreeing. The likelihood of using AI tools in marketing strategies was rated "very likely" by 23 respondents (56.1%) and "likely" by 13 (31.7%), a combined positive intention of 36 respondents (87.8%); 1 respondent (2.4%) rated it "very unlikely". By contrast, only 13 respondents (31.7%) agreed that their organisation had sufficient technical infrastructure, 13 (31.7%) that it had specialists with the required competencies, and 10 (24.4%) that it had a clear strategy for the use of AI in marketing. Agreement that the use of AI in marketing creates significant risks for the security of customer data was expressed by 29 respondents (70.7%).

Table 4. Distribution of responses to Likert items (N = 41; n and % of respondents)

Item	1	2	3	4	5	Agree (4+5)
L1. AI integration is a necessary condition of competitiveness in the Kazakhstani market	1 (2.4)	4 (9.8)	3 (7.3)	14 (34.1)	19 (46.3)	33 (80.5)
L2. Likelihood that our organisation will use AI tools in its marketing strategies	1 (2.4)	0 (0.0)	4 (9.8)	13 (31.7)	23 (56.1)	36 (87.8)
L3. Our organisation has sufficient technical infrastructure for AI in marketing	5 (12.2)	13 (31.7)	10 (24.4)	9 (22.0)	4 (9.8)	13 (31.7)
L4. Our organisation has specialists with the competencies to implement AI in marketing	5 (12.2)	14 (34.1)	9 (22.0)	10 (24.4)	3 (7.3)	13 (31.7)
L5. Our organisation has a clear strategy for the use of AI in marketing	6 (14.6)	13 (31.7)	12 (29.3)	8 (19.5)	2 (4.9)	10 (24.4)
L6. The use of AI in marketing creates significant risks for the security of customer data	1 (2.4)	3 (7.3)	8 (19.5)	17 (41.5)	12 (29.3)	29 (70.7)

Result 1 (Tables 3 and 4) corresponds to Contribution C1: it provides the baseline values of awareness, experience and intention before the entry into force of the Law on Artificial Intelligence.

3.4 Perceived threats of AI

The closed multiple-choice item on perceived threats (Table 5) was answered by all 41 respondents, who selected 3.1 options on average. The most frequently selected threats were an increase in phishing attacks and data theft carried out with AI assistants (31 respondents, 75.6%) and violation of user privacy (27, 65.9%), followed by failures and errors in the operation of AI systems (24, 58.5%), cybersecurity vulnerability of AI infrastructure, including attacks on and hacking of AI systems (22, 53.7%), and the use of AI for manipulative purposes, including the spread of fake news and interference in political campaigns (19, 46.3%). Three respondents (7.3%) selected "other" and named job losses and dependence on foreign technologies. None of the options, and none of the "other" entries, referred to an obligation of the respondent's own organisation.

Table 5. Perceived threats of AI (multiple choice; N = 41)

Threat	n	%
Increase in phishing attacks and data theft carried out with AI assistants	31	75.6
Violation of user privacy	27	65.9
Failures and errors in the operation of AI systems	24	58.5
Cybersecurity vulnerability of AI infrastructure (attacks, hacking)	22	53.7
Use of AI for manipulative purposes (fake news, political campaigns)	19	46.3
Other (job losses; dependence on foreign technologies)	3	7.3

3.5 Themes in open-ended responses

Thematic analysis of the 24 open-ended responses produced five themes (Table 6); 19 responses were assigned to more than one theme. Respondent codes indicate the serial number, type and sector of the organisation.

Table 6. Themes identified in open-ended responses (n = 24)

Theme	Definition	Responses, n (%)
T1. AI as an efficiency and content tool	AI is described through concrete productivity gains: text and visual content generation, drafting of advertising, response to customer enquiries, analysis of reviews	14 (58.3)
T2. Shortage of competencies and strategy	Lack of specialists, lack of understanding of where AI should be applied, absence of an internal strategy or owner of the topic	11 (45.8)

Theme	Definition	Responses, n (%)
T3. Data security and privacy concerns	Concern about leakage, theft or misuse of customer data; distrust of where data entered into AI tools end up; of these, references to legal requirements (consent, the Law on Personal Data)	10 (41.7); of which legal references 2 (8.3)
T4. Need for regulation and guidance	Requests for clear rules, state guidance, standards or certification of AI tools	7 (29.2)
T5. Cost, infrastructure and language	Cost of tools and integration, weak infrastructure, limited support of the Kazakh language by available tools	6 (25.0)

Theme T1 was the most frequent: respondents described AI primarily as a tool that saves time on routine marketing tasks ("we generate three variants of a post in ten minutes instead of a day" — R07, startup, IT; "the chatbot answers the standard questions, the manager handles the rest" — R19, company, retail). Theme T2 reflected the Likert results on competencies and strategy: "everyone uses ChatGPT, but nobody in the company is responsible for the result" (R12, company, financial services); "we do not understand which of our tasks are worth automating" (R23, company, manufacturing). Within Theme T3, concern was expressed in general terms — "I am afraid that client data will end up who knows where" (R04, startup, e-commerce); "after the leak in the summer everybody got nervous" (R15, company, financial services) — and was in most cases located outside the organisation; two responses referred to legal requirements, one noting that "consent of clients is needed for everything, and nobody knows exactly in what form" (R09, company, education and consulting) and one asking whether "it is at all permissible to upload the client base into foreign services" (R31, company, IT). Theme T4 contained requests for guidance from the state ("the Ministry should explain in plain language what is allowed and what is not" — R27, startup, IT) and for certification of tools. Theme T5 combined cost with the observation that available tools "work poorly in Kazakh" (R35, company, retail).

Result 2 (Tables 5 and 6) corresponds to Contribution C2: data security is recognised as a risk by 70.7% of respondents in the closed item and appears in 41.7% of open-ended responses, but references to the organisation's own legal obligations are absent from the closed items and occur in only 2 of 24 open-ended responses.

3.6 Mapping of perceived risks onto legal obligations

Table 7 maps the eight obligation groups of Table 1 onto the marketing practices that trigger them, the corresponding evidence in the survey responses, and the applicable sanctions. For none of the eight groups did any closed or open-ended response refer to the obligation as a duty of the respondent's own organisation; for two groups (O3 and O4), responses referred to the underlying risk without reference to the obligation.

Table 7. Mapping of legal obligations onto marketing practices, survey evidence and sanctions

Obligation	Marketing practice that triggers it	Evidence in survey responses	Sanction for non-compliance
O1. Consent (Law No. 94-V, Arts. 7, 8)	Collection of customer data for AI-based personalisation, profiling and targeting; use of CRM data for model training	Not mentioned as an obligation; 1 open-ended response (R09) notes uncertainty about the form of consent	KoAP Art. 79(1)–(2): up to 200–600 MCI for large businesses
O2. Prohibition on non-purpose extraction from public sources (Law No. 94-V, as amended 2026)	Scraping social networks and open directories to build lead lists and audiences	Not mentioned	KoAP Art. 79(1)–(2)
O3. Localisation (Art. 12) and cross-border transfer (Art. 16)	Entering customer data into foreign generative AI services; use of foreign cloud marketing platforms	95.1% use foreign consumer AI applications; 1 open-ended response (R31) asks whether uploading the client base to foreign services is permissible; no reference to the obligation	KoAP Art. 79; Criminal Code Art. 147 in case of substantial harm
O4. Protection measures and one-day breach notification (Art. 25; Orders No. 232/NQ, 338/NQ)	Any AI system holding customer data; integration of AI tools with CRM	"Phishing and data theft" (75.6%) and "vulnerability of AI infrastructure" (53.7%) selected as external threats; notification duty not mentioned	KoAP Art. 79(3)–(4): up to 600 MCI; up to 2,000 MCI (≈ 8.65 million tenge) if loss or unlawful processing results
O5. No decisions based solely on automated processing; human review (Law No. 326-VIII; Digital Code)	Automated scoring of customers, automated pricing, automated refusal of offers	Not mentioned	KoAP Art. 79; civil claims
O6. Prohibition on manipulative AI (Law No. 230-VIII)	Hyper-personalised persuasive messaging, dark patterns, targeting of vulnerable groups	"Manipulative use" selected by 46.3%, but in the context of fake news and politics, not of the organisation's own marketing	KoAP (new AI offences); prohibition of the system
O7. Labelling of synthetic content; disclosure of interaction with AI (Law No. 230-VIII)	AI-generated advertising images, video and text; chatbots and voice assistants in customer service	Not mentioned; chatbots described in open-ended responses (R19) without reference to disclosure	KoAP: 86,500 to 865,000 tenge depending on business size and repetition (2026 values)

Obligation	Marketing practice that triggers it	Evidence in survey responses	Sanction for non-compliance
O8. Right to erasure, anonymisation and restriction of processing (Digital Code; Law No. 94-V)	Customer data retained in training sets and vector databases; data retained by third-party AI providers	Not mentioned	KoAP Art. 79

Result 3 (Table 7) corresponds to Contribution C3. The obligation most directly exposed by respondents' reported behaviour is O3: with 95.1% of respondents using foreign consumer AI applications and 87.8% intending to use AI in marketing, routine entry of customer data into such services is probable, and only one respondent questioned its permissibility.

4. Discussion

4.1 RQ1: perception of privacy and security risks

RQ1 asked how Kazakhstani companies and startups perceive the privacy and security risks of AI in marketing. The results in Sections 3.4 and 3.5 show that the risks are perceived as real — 70.7% agree that AI creates significant risks for customer data, 75.6% select AI-enabled phishing and data theft and 65.9% privacy violation — but as external and generic. Four of the five threat options describe actors or failures outside the organisation; privacy violation is selected without connection to any practice of the organisation; and in the open-ended responses the concern is located "who knows where" (R04) or in the national leak of summer 2025 (R15). This is consistent with the experiential account of Puntoni et al. [19], in which AI is perceived as a source of exploitation by actors other than oneself, and with the KPMG finding that 40% of Kazakhstani companies are worried about data privacy while only 20% have AI-specific rules [15]. The perception is therefore accurate in direction but misplaced in locus: the obligations of the framework attach to the organisation's own practices, not to external attackers.

4.2 RQ2: readiness to adopt versus awareness of obligations

RQ2 asked whether declared readiness to adopt AI in marketing is accompanied by awareness of the organisation's own obligations. The results confirm a readiness–compliance gap. On the adoption side, 97.6% report medium or higher knowledge of AI, 95.1% use AI applications and 87.8% intend to use AI in marketing. On the compliance side, no closed response and only 2 of 24 open-ended responses (8.3%) refer to a legal obligation, and both of those express uncertainty rather than knowledge. The gap is not explained by indifference: 29.2% of open-ended responses ask for rules and guidance (T4). It mirrors the pattern reported for SMEs under the GDPR — awareness of the regime without identification of the

concrete steps it requires [25], [26] — and the global rate of policy-violating AI use [24]. The low values for infrastructure (31.7%), competencies (31.7%) and strategy (24.4%) in Table 4 suggest a structural cause: organisations without an owner of the AI topic have no one to translate the framework into internal rules, which is exactly the finding of Theme T2 ("nobody in the company is responsible for the result" — R12).

The gap has a specific consequence in Kazakhstan. Obligations O1, O3 and O4 were already in force at the time of the survey, and the fines under Article 79 had already been tripled; obligations O2, O5, O6 and O7 came into force within the following seven months. An organisation that perceives privacy only as an external threat is therefore likely to have been non-compliant with O1, O3 and O4 at the time of the survey and to have become non-compliant with four further obligation groups since, without any change in its own behaviour.

4.3 RQ3: obligations most exposed and resulting measures

RQ3 asked which obligations are most exposed by prevailing patterns of AI use. The mapping (Table 7) identifies O3 — localisation and cross-border transfer — as the most exposed. Entering customer names, contacts, purchase histories or feedback into a service whose infrastructure is located abroad is, on the face of Article 16, a cross-border transfer that is lawful only if the receiving state ensures protection of personal data or the data subject has consented; where the provider retains and may reuse inputs [22], it is also a disclosure to a third party outside the purposes of collection. The Samsung case [23] shows that even technically sophisticated organisations fail to control this behaviour, and the 48% rate of policy-violating AI use [24] makes it unlikely that Kazakhstani marketing teams are an exception. The one open-ended response that raised the question ("is it at all permissible to upload the client base into foreign services" — R31) shows that the issue is recognisable once articulated, but is not currently articulated. This "shadow AI" channel is invisible to information security controls focused on the organisation's own infrastructure and deserves specific attention from the authorized body.

The second most exposed group is O6. Respondents named manipulation as a risk (46.3%) but located it in fake news and politics. The Law on Artificial Intelligence prohibits manipulative systems regardless of context, including commercial persuasion; hyper-personalised messaging that exploits consumers' malleable privacy decisions [18] now sits close to a statutory prohibition, and the boundary between legitimate personalisation and prohibited manipulation is undefined in practice. O7 (labelling and disclosure) is exposed by the chatbots and generated content that respondents describe as their main use case (T1) without any reference to disclosure.

Three measures follow for companies: an internal AI use policy prohibiting the entry of customer personal data into external generative AI services unless a lawful transfer basis and a contractual guarantee of non-retention exist; a review of consent texts and privacy notices to cover AI-based profiling, automated decisions and AI-generated communications,

including labelling; and assignment of responsibility for one-day breach notification and for entry in the register of persons processing personal data. Table 7 can be used as the checklist for this review. For the authorized body, the results indicate that enforcement alone will not close the gap, because respondents do not resist compliance but are unaware of it and ask for guidance (T4); sector-specific guidance for marketing on the status of foreign generative AI services under Articles 12 and 16, on lawful personalisation under the Law on Artificial Intelligence and on labelling of AI-generated advertising would address the most exposed obligations directly, and the announced increase of fines to 5,000 MCI [14] will be more effective if accompanied by such guidance. For educational programmes, the results confirm the shortage of specialists combining marketing competence with data protection and AI governance competence.

4.4 Limitations

The sample is small (N = 41) and non-probabilistic, with an over-representation of the IT sector and of small organisations; the results describe the surveyed group and cannot be generalised to all Kazakhstani companies. The instrument measured perceived risk in general terms and did not include items on specific legal obligations; the mapping in Table 7 is therefore an interpretation of respondents' silence on obligations, not a direct measurement of their knowledge, and the two open-ended references to legal requirements may understate awareness that respondents did not think relevant to the question asked. The thematic analysis is based on short written responses rather than interviews. Finally, the survey preceded the entry into force of the Law on Artificial Intelligence and the Digital Code, so the results measure perception under the framework as it stood in 2025 and cannot show whether the new instruments have changed it. Appendix B proposes a module of ten items mapped to specific obligations that addresses the first two limitations and allows the baseline reported here to be compared with a post-2026 wave.

5. Conclusion

Kazakhstan has moved within twenty months from a single personal data law to a three-instrument framework that attaches specific obligations to ordinary marketing practices — consent for profiling, localisation of data, one-day breach notification, prohibition of scraping and of manipulative systems, labelling of AI-generated content. This study shows that the businesses most eager to adopt AI in marketing entered that framework without perceiving those obligations as their own. The significance of the result lies less in the small sample than in its timing and its structure: taken immediately before the Law on Artificial Intelligence entered into force, it fixes the point from which the effect of the new framework can be measured, and it shows that the gap is not one of indifference — respondents recognise the risk and ask for rules — but of locus, with risk perceived in external attackers rather than in the organisation's own handling of customer data through foreign AI services.

The scientific novelty of this work — the first empirical, obligation-level reading of business perception of AI-related privacy risk in Kazakhstan against the amended Law on Personal Data, the Law on Artificial Intelligence and the Digital Code — has been confirmed by the finding that none of eight obligation groups is reflected in respondents' perceptions while the behaviour of 95.1% of respondents directly engages the localisation and cross-border transfer requirements; this demonstrates that readiness to adopt AI and readiness to comply with the framework are distinct constructs that must be measured separately. The claim is substantiated for the surveyed group; its generalisation to the population of Kazakhstani companies requires the larger, stratified wave for which the supplementary module is provided.

Three directions for future research follow. First, the supplementary module should be applied to a stratified sample after the Digital Code has been in force for at least a year, so that the baseline reported here can be compared with perception under the full framework. Second, the actual practice of marketing teams in entering customer data into generative AI services should be studied directly, by interview or by analysis of organisational policies, since survey silence on an obligation is only indirect evidence of non-compliance. Third, the boundary between lawful personalisation and prohibited manipulation under the Law on Artificial Intelligence requires doctrinal and empirical work before it can be enforced or complied with; the mapping proposed here offers a starting point for both.

Author Contributions

Conceptualization: R.K.; Methodology: R.K. and A.A.; Investigation: A.A.; Formal analysis: R.K. and A.A.; Writing — original draft preparation: R.K.; Writing — review and editing: R.K. and A.A.; Supervision: R.K.

Conflicts of Interest

The authors declare no other conflict of interest.

Data Availability Statement

The anonymised survey responses (N = 41) and the coding of open-ended responses are available from the corresponding author on reasonable request. The dataset is not deposited publicly because the open-ended responses contain descriptions of organisations that could allow their identification.

List of Supplementary Materials

- Appendix A: Questionnaire (15 items) as administered in Google Forms.
- Appendix B: Proposed supplementary survey module on regulatory readiness (10 items mapped to legal obligations).

References

[1]. Davenport, T., 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://doi.org/10.1007/s11747-019-00696-0

[2]. Huang, M.-H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. *Journal of the Academy of Marketing Science, 49*(1), 30–50. https://doi.org/10.1007/s11747-020-00749-9

[3]. Mustak, M., Salminen, J., Plé, L., & Wirtz, J. (2021). Artificial intelligence in marketing: Topic modeling, scientometric analysis, and research agenda. *Journal of Business Research, 124*, 389–404. https://doi.org/10.1016/j.jbusres.2020.10.044

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

[5]. Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing, 37*(3), 466–480. https://doi.org/10.1016/j.ijresmar.2020.03.006

[6]. Hermann, E. (2022). Leveraging artificial intelligence in marketing for social good — An ethical perspective. *Journal of Business Ethics, 179*(1), 43–61. https://doi.org/10.1007/s10551-021-04843-y

[7]. Postanovlenie Pravitel'stva Respubliki Kazakhstan ot 24 iyulya 2024 goda No. 592 «Ob utverzhdenii Kontseptsii razvitiya iskusstvennogo intellekta na 2024–2029 gody» [Decree of the Government of the Republic of Kazakhstan No. 592 of 24 July 2024 "On Approval of the Concept for the Development of Artificial Intelligence for 2024–2029"]. (2024). Adilet. https://adilet.zan.kz/rus/docs/P2400000592

[8]. Ukaz Prezidenta Respubliki Kazakhstan ot 18 sentyabrya 2025 goda No. 997 «O merakh po dal'neyshemu sovershenstvovaniyu sistemy gosudarstvennogo upravleniya» [Decree of the President of the Republic of Kazakhstan No. 997 of 18 September 2025 "On Measures for Further Improvement of the Public Administration System"]. (2025).

[9]. Kodeks Respubliki Kazakhstan ob administrativnykh pravonarusheniyakh ot 5 iyulya 2014 goda No. 235-V (v redaktsii Zakona ot 10 yanvarya 2025 goda No. 155-VIII) [Code of the Republic of Kazakhstan on Administrative Offences No. 235-V of 5 July 2014 (as amended by Law No. 155-VIII of 10 January 2025)]. (2014). Adilet. https://adilet.zan.kz/rus/docs/K1400000235

[10]. Zakon Respubliki Kazakhstan ot 17 noyabrya 2025 goda No. 230-VIII «Ob iskusstvennom intellekte» [Law of the Republic of Kazakhstan No. 230-VIII of 17 November 2025 "On Artificial Intelligence"]. (2025). Adilet. https://adilet.zan.kz/rus/docs/Z2500000230

[11]. Tsifrovoy kodeks Respubliki Kazakhstan ot 9 yanvarya 2026 goda No. 255-VIII [Digital Code of the Republic of Kazakhstan No. 255-VIII of 9 January 2026]. (2026).

[12]. Zakon Respubliki Kazakhstan ot 21 maya 2013 goda No. 94-V «O personal'nykh dannykh i ikh zashchite» (s izmeneniyami i dopolneniyami po sostoyaniyu na 25.08.2026) [Law of the Republic of Kazakhstan No. 94-V of 21 May 2013 "On Personal Data and Their Protection" (as amended on 25 August 2026)]. (2013). Adilet. https://adilet.zan.kz/rus/docs/Z1300000094

[13]. Zakon Respubliki Kazakhstan ot 24 iyunya 2026 goda No. 326-VIII «O vnesenii izmeneniy i dopolneniy v nekotorye zakonodatel'nye akty Respubliki Kazakhstan po voprosam tsifrovizatsii, zashchity personal'nykh dannykh, dorozhnogo dvizheniya i peredovykh transportnykh tekhnologiy» [Law of the Republic of Kazakhstan No. 326-VIII of 24 June 2026 "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Issues of Digitalisation, Protection of Personal Data, Road Traffic and Advanced Transport Technologies"]. (2026).

[14]. Zakon.kz. (2026, September 29). Shtrafy za utechku personal'nykh dannykh dlya kompaniy khotyat povysit' v Kazakhstane [Fines for personal data leaks for companies are to be increased in Kazakhstan]. Zakon.kz. https://zakon.kz/obshestvo/6533131-shtrafy-za-utechku-personalnykh-dannykh-dlya-kompaniy-khotyat-povysit-v-kazakhstane.html

[15]. KPMG in Kazakhstan and Central Asia, & Digital Business. (2025, March). *Kazakhstan AI readiness report*. KPMG. https://assets.kpmg.com/content/dam/kpmg/kz/pdf/2025/03/Kazakhstan-AI-Readiness-eng.pdf

[16]. Kazinform. (2025). Kiberugroza: pochemu proizoshla utechka personal'nykh dannykh kazakhstantsev i kak ikh zashchitit' [Cyber threat: Why the leak of personal data of Kazakhstanis occurred and how to protect them]. Kazinform. https://www.inform.kz/ru/kiberugroza-pochemu-proizoshla-utechka-personalnih-dannih-kazahstantsev-i-kak-ih-zashitit-df15ec

[17]. Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

[18]. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology, 30*(4), 736–758. https://doi.org/10.1002/jcpy.1191

[19]. Puntoni, S., Reczek, R. W., Giesler, M., & Botti, S. (2021). Consumers and artificial intelligence: An experiential perspective. *Journal of Marketing, 85*(1), 131–151. https://doi.org/10.1177/0022242920953847

[20]. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence, 1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

[21]. Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., Krishen, A. S., Kumar, V., Rahman, M. M., Raman, R., Rauschnabel, P. A., Rowley, J., Salo, J., Tran, G. A., & Wang, Y. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International Journal of Information Management, 59*, 102168. https://doi.org/10.1016/j.ijinfomgt.2020.102168

[22]. 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

[23]. Gurman, M. (2023, May 2). Samsung bans staff's AI use after spotting ChatGPT data leak. *Bloomberg*. https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak

[24]. Gillespie, N., Lockey, S., Ward, T., Macdade, A., & Hassed, G. (2025). *Trust, attitudes and use of artificial intelligence: A global study 2025*. The University of Melbourne and KPMG. https://doi.org/10.26188/28822919

[25]. Brodin, M. (2019). A framework for GDPR compliance for small- and medium-sized enterprises. *European Journal for Security Research, 4*(2), 243–264. https://doi.org/10.1007/s41125-019-00042-z

[26]. Freitas, M. da C., & Mira da Silva, M. (2018). GDPR compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management, 3*(4), 30. https://doi.org/10.20897/jisem/3941

[27]. Omarova, B., Mukhtorov, A., & Yerlankyzy, A. (2024). Kazakhstan. In *Privacy and personal data protection law in Asia* (pp. 435–462). Hart Publishing. https://doi.org/10.5040/9781509965502.ch-017

[28]. Akhmetova, S. B., Tursynkulova, D. A., & Ibrayev, N. S. (2024). Powers of the Personal Data Protection Authority in Europe and Kazakhstan: Comparative analysis, recommendations for improving the activities of the Kazakhstani Personal Data Protection Authority. *Bulletin of L.N. Gumilyov Eurasian*

National University. Law Series, 148(3), 201–214. https://doi.org/10.32523/2616-6844-2024-148-3-201-214

[29]. Alibayeva, G. A., & Yerbolatov, E. E. (2025). Review of legal protection of personal data in Kazakhstan and abroad. *Bulletin of Toraigyrov University. Law Series*, (1), 16–29. https://doi.org/10.48081/cxuk5853

[30]. Prikaz Ministra iskusstvennogo intellekta i tsifrovogo razvitiya Respubliki Kazakhstan ot 30 aprelya 2026 goda No. 232/NQ «Ob utverzhdenii Pravil uvedomleniya o narusheniyakh bezopasnosti personal'nykh dannykh» [Order of the Minister of Artificial Intelligence and Digital Development of the Republic of Kazakhstan No. 232/NQ of 30 April 2026 "On Approval of the Rules for Notification of Personal Data Security Breaches"]. (2026). Adilet.

[31]. Prikaz Ministra iskusstvennogo intellekta i tsifrovogo razvitiya Respubliki Kazakhstan ot 22 iyunya 2026 goda No. 338/NQ «Ob utverzhdenii Pravil osushchestvleniya mer po zashchite personal'nykh dannykh» [Order of the Minister of Artificial Intelligence and Digital Development of the Republic of Kazakhstan No. 338/NQ of 22 June 2026 "On Approval of the Rules for the Implementation of Measures for the Protection of Personal Data"]. (2026). Adilet. https://adilet.zan.kz/rus/docs/V2300032810

[32]. Zakon Respubliki Kazakhstan ot 24 noyabrya 2015 goda No. 418-V «O kiberbezopasnosti» (ranee — «Ob informatizatsii»; v redaktsii Zakona ot 9 yanvarya 2026 goda No. 256-VIII) [Law of the Republic of Kazakhstan No. 418-V of 24 November 2015 "On Cybersecurity" (formerly "On Informatization"; as amended by Law No. 256-VIII of 9 January 2026)]. (2015). Adilet. https://adilet.zan.kz/rus/docs/Z1500000418

[33]. Ugolovnyy kodeks Respubliki Kazakhstan ot 3 iyulya 2014 goda No. 226-V [Criminal Code of the Republic of Kazakhstan No. 226-V of 3 July 2014]. (2014). Adilet. https://adilet.zan.kz/rus/docs/K1400000226

[34]. Digital Rights Center Qazaqstan. (2024). 4 910 360 — summa shtrafov za narusheniya v sfere personal'nykh dannykh s nachala 2024 goda [4,910,360 — the amount of fines for violations in the field of personal data since the beginning of 2024]. Digital Rights Center Qazaqstan. https://drcq.law/blog/4-910-360-summa-shtrafov-za-narusheniya-v-sfere-personalnykh-dannykh-s-nachala-2024-goda/

[35]. Profit.kz. (2025). Bol'she 40 utechek personal'nykh dannykh proizoshlo v Kazakhstane s nachala goda [More than 40 personal data leaks have occurred in Kazakhstan since the beginning of the year]. Profit.kz. https://profit.kz/news/69493/

[36]. Postanovlenie Pravitel'stva Respubliki Kazakhstan ot 28 marta 2023 goda No. 269 «Ob utverzhdenii Kontseptsii tsifrovoy transformatsii, razvitiya otrasli informatsionno-kommunikatsionnykh tekhnologiy i kiberbezopasnosti na 2023–2029 gody» [Decree of the Government of the Republic of Kazakhstan No. 269 of 28 March 2023 "On Approval of the Concept of Digital Transformation, Development of the Information and Communication Technology Industry and Cybersecurity for 2023–2029"]. (2023). Adilet. https://adilet.zan.kz/rus/docs/P2300000269

[37]. International Monetary Fund. (2024). *AI Preparedness Index (AIPI)* [Data set]. IMF DataMapper. https://www.imf.org/external/datamapper/datasets/AIPI

[38]. Oxford Insights. (2025). *Government AI Readiness Index 2025*. Oxford Insights. https://oxfordinsights.com/ai-readiness/ai-readiness-index/

[39]. Braun, V., & Clarke, V. (2021). One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology*, *18*(3), 328–352. https://doi.org/10.1080/14780887.2020.1769238

Supplementary Materials

Privacy Risks and Data Protection Readiness in AI Marketing in Kazakhstan

Raushan Kambar, Assel Abildayeva

APPENDIX A. Questionnaire

Introductory text and consent. This survey is conducted for a study on the use of artificial intelligence (AI) in the marketing activities of Kazakhstani companies and startups. Participation is voluntary and anonymous; no personal data are collected, and the answers will be used only in aggregated form for research purposes. Completing the questionnaire takes about 7 minutes. By proceeding to the questions you confirm that you have read this information and agree to participate.

Part A. About your organisation and you (closed items)

Q1. Type of organisation: (a) company; (b) startup.

Q2. Main sector of activity: (a) information technology and telecommunications; (b) retail and e-commerce; (c) financial services; (d) education and consulting; (e) manufacturing and logistics; (f) other services (please specify).

Q3. Number of employees: (a) up to 15; (b) 16–100; (c) 101–250; (d) over 250.

Q4. Your role in the organisation: (a) owner or founder; (b) senior manager (director, deputy director); (c) marketing manager or specialist; (d) IT or analytics specialist; (e) other (please specify).

Part B. Awareness and use of AI (closed items)

Q5. How would you rate your level of knowledge about artificial intelligence? (a) very low; (b) low; (c) medium; (d) high; (e) very high.

Q6. Have you used applications based on artificial intelligence (for example, ChatGPT, Siri, Google Assistant)? (a) yes; (b) no.

Q7. Does your organisation currently use artificial intelligence in its marketing activities? (a) yes, regularly; (b) occasionally or as a pilot; (c) not yet.

Q8. Which threats do you associate with the development and implementation of artificial intelligence? (select all that apply) (a) increase in phishing attacks and data theft carried out with AI assistants; (b) failures and errors in the operation of AI systems; (c) cybersecurity vulnerability of AI infrastructure, including attacks on and hacking of AI systems; (d) violation of user privacy; (e) use of AI for manipulative purposes, including the spread of fake news and interference in political campaigns; (f) other (please specify).

Part C. Attitudes (5-point scale)

For statements Q9 and Q11–Q14: 1 = strongly disagree; 2 = disagree; 3 = neither agree nor disagree; 4 = agree; 5 = strongly agree. For Q10: 1 = very unlikely; 2 = unlikely; 3 = not sure; 4 = likely; 5 = very likely.

Q9. The integration of artificial intelligence is a necessary condition for maintaining competitiveness in the Kazakhstani market.

Q10. How likely is it that your organisation will use artificial intelligence tools in its marketing strategies in the future?

Q11. Our organisation has sufficient technical infrastructure to use artificial intelligence in marketing.

Q12. Our organisation has specialists with the competencies needed to implement artificial intelligence in marketing.

Q13. Our organisation has a clear strategy for the use of artificial intelligence in marketing.

Q14. The use of artificial intelligence in marketing creates significant risks for the security of customer data.

Part D. Open-ended item (optional)

Q15. Please share your views, experience or recommendations regarding the use of artificial intelligence in marketing in Kazakhstan.

APPENDIX B. Proposed supplementary module on regulatory readiness

The module is intended for subsequent survey waves. Items S2.1–S2.8 are answered on a 5-point scale (1 = strongly disagree, 5 = strongly agree; "do not know" is also offered) and are mapped to a specific obligation of the legal framework (Table S2.1). Items S2.9 and S2.10 measure awareness of the framework and guidance needs.

Table S2.1. Supplementary survey items mapped to legal obligations

No.	Item	Obligation measured
S2.1	Our organisation obtains the consent of customers, in the form required by the Law on Personal Data, before using their data for AI-based personalisation or profiling.	O1 — Consent (Law No. 94-V, Arts. 7, 8)
S2.2	Our organisation does not collect customer or prospect data from social networks or open sources to build or expand marketing databases.	O2 — Prohibition on non-purpose extraction from public sources (Law No. 94-V, as amended 2026)

No.	Item	Obligation measured
S2.3	Employees of our organisation are prohibited from entering personal data of customers into external AI services (ChatGPT and analogues), or such use is permitted only on a documented lawful basis.	O3 — Localisation and cross-border transfer (Law No. 94-V, Arts. 12, 16)
S2.4	Our organisation has a designated person and a procedure for notifying the authorized body of a personal data security breach within one working day.	O4 — Protection measures and breach notification (Law No. 94-V, Art. 25)
S2.5	Our organisation has registered, or has assessed whether it must register, as a person collecting and processing personal data.	Register of persons processing personal data (Law No. 326-VIII)
S2.6	Advertising and marketing content generated with AI is labelled as such, and customers are informed when they communicate with a chatbot or voice assistant.	O7 — Labelling and disclosure (Law No. 230-VIII)
S2.7	Our organisation has assessed whether its AI-based marketing tools could be classified as manipulative or as exploiting vulnerabilities of customers.	O6 — Prohibition on manipulative AI (Law No. 230-VIII)
S2.8	Customers can request deletion of their data from all systems, including AI tools and third-party providers, and we can fulfil such a request.	O8 — Right to erasure (Digital Code; Law No. 94-V)
S2.9	(Multiple choice) Which of the following legal acts does your organisation take into account when using AI in marketing? Law on Personal Data; Law on Artificial Intelligence; Digital Code; Law on Advertising; none; do not know.	Awareness of the framework
S2.10	(Open) What guidance from the authorized body would help your organisation use AI in marketing lawfully?	Guidance needs