



## Legal aspects of digital marketing: A comprehensive analysis of data collection, storage, and usage practices in Uzbekistan

Azam Sarabekov

Researcher, Department Private International Law, Tashkent State University of Law, Uzbekistan

### Abstract

This article offers an in-depth examination of the legal dimensions of digital marketing in Uzbekistan, emphasizing data collecting, storage, and utilization methods. It analyzes the existing legal framework regulating these behaviors, encompassing the Law on Personal Data and the Law on Advertising, and proposes potential areas for enhancement. The research underscores significant difficulties like informed consent, data security, transnational data transfers, targeted advertising, and personalization. The article proposes prospective reforms to improve consumer safety and promote innovation in the digital economy by drawing analogies with international regulations such as the EU's General Data Safety Regulation (GDPR). This encompasses implementing stricter data security standards, establishing explicit regulations for cross-border data transfers and targeted advertising, and formulating a more extensive accountability framework for data protection infringements. The study continues by underscoring the necessity for continuous collaboration among policymakers, industry stakeholders, and consumer advocates to establish a balanced legal framework that tackles the increasing issues of digital marketing.

**Keywords:** Digital marketing, data protection, privacy, Uzbekistan, GDPR, consumer rights, data security, targeted advertising, legal liability, cross-border data transfers, personalization, data collection, data storage, data usage, legal framework

### Introduction

Digital marketing has become an integral part of the modern digital economy, revolutionizing the way businesses interact with and engage their customers. At the core of digital marketing lies the collection, storage, and utilization of consumer data, which enables targeted advertising, personalized experiences, and data-driven decision-making<sup>[1]</sup>. However, the rapid growth of digital marketing has also raised significant legal and ethical concerns regarding consumer privacy, data security, and the potential for misuse or abuse of personal information<sup>[2]</sup>. This article aims to provide a comprehensive analysis of the legal aspects of digital marketing in Uzbekistan, focusing on the existing legal frameworks, international standards, and potential areas for improvement. By examining the key issues surrounding data collection, storage, and usage in digital marketing, this article seeks to contribute to the ongoing discourse on balancing the benefits of digital marketing with the protection of consumer rights and privacy.

### Main researches and analyses

The collection of consumer data forms the foundation of digital marketing strategies, enabling businesses to gain valuable insights into consumer preferences, behaviors, and demographics<sup>[3]</sup>. In Uzbekistan, the legal framework governing data collection in digital marketing is primarily governed by the Law on Personal Data, which sets out the principles and requirements for the processing of personal data<sup>[4]</sup>. However, the current legal provisions may not adequately address the specific challenges posed by digital marketing, such as the issue of informed consent and the potential for data misuse.

A primary concern about data acquisition in digital marketing is the concept of informed consent. The Law on Personal Data mandates that data controllers secure consent

from individuals prior to the collection and processing of their personal data; nevertheless, the practical execution of this obligation in digital marketing poses significant challenges. Numerous consumers may lack a comprehensive understanding of the ramifications of granting their consent or may be unable to make an informed decision due to the intricacy and length of privacy policies and terms of service. This underscores the necessity for more transparent and user-centric methods for acquiring informed permission, including explicit and succinct privacy notifications, opt-in/opt-out alternatives, and detailed control over data sharing choices.

Furthermore, the existing regulatory framework in Uzbekistan may insufficiently mitigate the risks of data misuse or unlawful access to personal information obtained via digital marketing channels. The Law on Personal Data establishes specific safeguards, including the obligation for data controllers to adopt suitable technical and organizational measures to secure personal data. Nonetheless, the swift advancement of digital marketing technology and the growing complexity of cyber risks may require a more thorough and flexible strategy for data protection.

To address these challenges, Uzbekistan could consider adopting a more comprehensive data protection framework, drawing inspiration from international best practices such as the European Union's General Data Protection Regulation (GDPR)<sup>[5]</sup>. The GDPR sets a high standard for data protection, emphasizing principles such as data minimization, purpose limitation, and data subject rights, which could serve as a model for enhancing the legal framework in Uzbekistan. Additionally, the development of industry-specific guidelines and codes of conduct could help to promote responsible data collection practices and foster trust between businesses and consumers.

The storage of consumer data collected through digital marketing activities raises significant legal and ethical concerns, particularly in relation to data security and confidentiality. In Uzbekistan, the Law on Personal Data establishes general requirements for the storage and protection of personal data, obligating data controllers to implement appropriate technical and organizational measures to ensure the security of personal data <sup>[6]</sup>. However, the rapid advancement of digital technologies and the increasing complexity of data storage solutions may require a more nuanced and adaptive approach to data protection.

A primary concern in safeguarding the security and confidentiality of customer data is the risk of unauthorized access or data breaches. In digital marketing, the accumulation and storage of extensive personal information render the repercussions of a data breach graver, resulting in identity theft, financial fraud, and reputational harm. To mitigate these dangers, firms involved in digital marketing must have stringent data security protocols, including encryption, access limits, and periodic security audits.

However, the current legal framework in Uzbekistan may not provide sufficient guidance or incentives for businesses to implement such measures. While the Law on Personal Data does require data controllers to ensure the security of personal data, it does not prescribe specific technical or organizational measures that must be adopted <sup>[6]</sup>. This lack of specificity may lead to inconsistent or inadequate data protection practices across different businesses and sectors.

To address these challenges, Uzbekistan could consider adopting more specific and stringent data security requirements, drawing inspiration from international standards and best practices. For example, the Payment Card Industry Data Security Standard (PCI DSS) sets out detailed requirements for the secure storage and processing of payment card data, which could serve as a model for developing industry-specific data security standards in Uzbekistan <sup>[7]</sup>. Additionally, the introduction of mandatory data breach notification requirements, similar to those found in the GDPR, could help to promote transparency and accountability in the event of a data security incident <sup>[8]</sup>.

An further significant consideration regarding data storage and secrecy is the matter of cross-border data transfers. In digital marketing, consumer data may be transmitted internationally for processing or as part of global marketing initiatives. The existing legislative framework in Uzbekistan lacks explicit standards or limitations for cross-border data transfers, thereby subjecting consumer data to heightened risks or jurisdictional ambiguities.

To address this issue, Uzbekistan could consider adopting specific provisions on cross-border data transfers, similar to those found in the GDPR. The GDPR requires that personal data may only be transferred to countries outside the European Union if certain conditions are met, such as the existence of an adequacy decision or the implementation of appropriate safeguards <sup>[8]</sup>. By adopting similar provisions, Uzbekistan could help to ensure that consumer data is afforded an adequate level of protection even when transferred outside the country.

The usage of consumer data in digital marketing raises a range of legal and ethical concerns, particularly in relation to targeted advertising, personalization, and the potential for discriminatory practices. In Uzbekistan, the legal framework governing data usage in digital marketing is primarily

governed by the Law on Advertising, which sets out general principles and requirements for advertising activities <sup>[9]</sup>. However, the current legal provisions may not adequately address the specific challenges posed by data-driven digital marketing practices.

One of the key concerns surrounding data usage in digital marketing is the issue of targeted advertising. Targeted advertising involves the use of consumer data to deliver personalized advertising content based on an individual's preferences, behaviors, or demographics <sup>[10]</sup>. While targeted advertising can be beneficial for both businesses and consumers, enabling more relevant and engaging advertising experiences, it also raises significant privacy concerns. Consumers may feel that their personal information is being exploited for commercial purposes, or that they are being subjected to intrusive or manipulative advertising practices <sup>[11]</sup>.

To address these concerns, Uzbekistan could consider adopting specific provisions on targeted advertising, drawing inspiration from international best practices. For example, the GDPR requires that targeted advertising may only be conducted with the explicit consent of the individual, and that individuals must be provided with clear and concise information about the processing of their personal data for advertising purposes <sup>[12]</sup>. Additionally, the GDPR grants individuals the right to object to the processing of their personal data for direct marketing purposes, including targeted advertising.

Another important aspect of data usage in digital marketing is the issue of personalization. Personalization involves the use of consumer data to tailor products, services, or content to an individual's specific preferences or characteristics <sup>[13]</sup>. While personalization can enhance the consumer experience and drive engagement, it also raises concerns about the potential for discriminatory practices or the reinforcement of existing biases.

To mitigate these risks, Uzbekistan could consider adopting specific provisions on the use of automated decision-making and profiling in the context of digital marketing. The GDPR, for example, grants individuals the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects or similarly significant impacts <sup>[8]</sup>. By adopting similar provisions, Uzbekistan could help to ensure that consumers are protected against potentially harmful or discriminatory practices arising from the use of automated decision-making in digital marketing.

The matter of legal accountability for breaches of data protection and privacy regulations in digital marketing is crucial, as it ensures that organizations are accountable for their data gathering, storage, and utilization methods. The legal framework in Uzbekistan regarding accountability for data privacy violations is principally dictated by the Code of Administrative Responsibility and the Criminal Code, which delineate penalties for offenses linked to the abuse or unauthorized disclosure of personal data <sup>[14]</sup>.

Nevertheless, the existing regulatory frameworks may insufficiently tackle the distinct difficulties presented by digital marketing, like the risk of extensive data breaches or the exploitation of customer data for targeted advertising. Recent years have witnessed numerous prominent instances of data breaches and privacy infringements within digital marketing, underscoring the necessity for more stringent enforcement procedures and deterrent punishments.

To address these challenges, Uzbekistan could consider adopting a more comprehensive and stringent liability regime for data protection violations in the context of digital marketing. This could include the introduction of higher fines for serious violations, similar to those found in the GDPR, which can reach up to 4% of a company's global annual turnover <sup>[8]</sup>. Additionally, the introduction of a private right of action, allowing individuals to seek compensation for damages suffered as a result of data protection violations, could help to promote greater accountability and redress for consumers.

An further significant facet of legal liability in digital marketing pertains to the matter of cross-border enforcement. Due to the international scope of digital marketing, it is imperative that data protection authorities collaborate efficiently across borders to investigate and prosecute infringements. Uzbekistan may contemplate ratifying international accords on data protection and privacy, including the Council of Europe's Convention 108+ or the OECD Privacy Guidelines <sup>[15]</sup>.

Furthermore, establishing a robust and autonomous data protection body, equipped with sufficient resources and enforcement capabilities, is essential for guaranteeing effective oversight and adherence to data protection regulations in the realm of digital marketing. The data protection authority must be authorized to do investigations, issue enforceable directives, and apply sanctions for infractions, in addition to offering advise and assistance to enterprises and customers regarding data protection matters.

The swift advancement of digital marketing technologies and methodologies poses both potential and concerns for the legal control of data collecting, storage, and use in Uzbekistan. To maintain the efficacy and adaptability of the legal framework in digital marketing, it is crucial to identify possible areas for enhancement and reform.

A primary area for enhancement is the alignment of data protection laws and standards across various sectors and jurisdictions. Due to the worldwide scope of digital marketing, it is essential for businesses to function within a uniform and reliable regulatory framework, while also guaranteeing that customers receive sufficient protection irrespective of the location of their data processing. Uzbekistan might enhance its data protection legislation by matching them more closely with international standards and best practices, such as the GDPR or the APEC Privacy Framework.

A further potential area for enhancement is the formulation of industry-specific norms and codes of behavior for digital marketing. These principles could facilitate ethical data collection and usage practices, while also offering enterprises enhanced clarity and certainty over their legal obligations. The formulation of these recommendations may be executed in partnership with industry players, consumer advocacy organizations, and academic authorities, to guarantee a balance between company interests and consumer rights.

Furthermore, the legal framework might be enhanced by incorporating more comprehensive data subject rights, including the right to data portability and the right to an explanation for automated decision-making. These rights may allow customers to exert more control over their personal data, while simultaneously fostering increased

transparency and accountability in the application of algorithms and artificial intelligence in digital marketing.

Moreover, the legal structure could be improved by establishing more efficient conflict resolution methods, like alternative dispute resolution (ADR) or online dispute resolution (ODR) platforms. These procedures may offer consumers more accessible and efficient avenues for obtaining remedy for data privacy infringements, thereby alleviating the strain on the judicial system.

It is imperative that the legal foundation for digital marketing is bolstered by continuous education and awareness initiatives to ensure that firms and consumers are cognizant of their rights and responsibilities under data protection legislation. This may encompass the creation of public awareness initiatives, the provision of training and resources for enterprises, and the integration of data protection and privacy concerns into educational programs.

## Conclusion

In summary, the legal dimensions of digital marketing in Uzbekistan constitute a complex and dynamic environment, with considerable ramifications for the safeguarding of consumer rights and privacy. The existing legislative framework establishes a basis for regulating data collection, storage, and usage practices; yet, substantial opportunities for enhancement and reform persist.

To maintain the efficacy and adaptability of the legal framework in the evolving realm of digital marketing, it is imperative to contemplate various potential measures, such as the harmonization of data protection laws and standards, the formulation of industry-specific guidelines and codes of conduct, the establishment of more stringent data subject rights, the creation of effective dispute resolution mechanisms, and the continuation of educational and awareness initiatives.

Uzbekistan may foster the growth and innovation of the digital economy by adopting a proactive and comprehensive legal framework for digital marketing, while simultaneously safeguarding the rights and interests of consumers. As the digital landscape evolves, it is crucial for policymakers, industry stakeholders, and consumer advocates to collaborate in establishing a legislative framework that reconciles the advantages of digital marketing with the necessity of protecting personal data and privacy.

## References

1. Kotler P, Kartajaya H, Setiawan I, Marketing 5.0: Technology for humanity. John Wiley Sons, 2021.
2. Nair, A. The dark side of digital marketing: Ethics and privacy concerns. *International Journal of Advanced Science Technology*,2020;29(5):2875-2884.
3. Wedel M, Kannan PK. Marketing analytics for data-rich environments. *Journal of Marketing*,2016;80(6):97-121.
4. Law of the Republic of Uzbekistan On Personal Data. Retrieved, 2019. from <https://lex.uz/docs/4396428>
5. Regulation EU 2016/679 of the European Parliament and of the Council of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC General Data Protection Regulation. *Official Journal of the European Union*,2016;119:1-88.

6. Law of the Republic of Uzbekistan On Personal Data, Retrieved, 2019,15. from <https://lex.uz/docs/4396428>
7. Payment Card Industry Security Standards Council. Payment Card Industry PCI Data Security Standard: Requirements and Security Assessment Procedures, Version 3.2.1. Retrieved, 2018 from [https://www.pcisecuritystandards.org/document\\_library](https://www.pcisecuritystandards.org/document_library)
8. Regulation EU 2016/679 of the European Parliament and of the Council of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC General Data Protection Regulation, Official Journal of the European Union,2016:119:1-88.
9. Law of the Republic of Uzbekistan On Advertising Retrieved, 1998. from <https://lex.uz/docs/4672817>
10. Boerman SC, Kruikemeier S, Zuiderveen Borgesius FJ. Online behavioral advertising A literature review research agenda. Journal of Advertising,2017;46(3):363-376.
11. Babayev J. Safeguarding Consumer Rights in the Digital Age Challenges Strategies. Uzbek Journal of Law and Digital Policy, 2023, 1-11.
12. Regulation EU. 2016/679 of the European Parliament and of the Council of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC General Data Protection Regulation, Article 22. Official Journal of the European Union,2016:119:1-88.
13. Vesanen J. What is personalization A conceptual framework. European Journal of Marketing,2007;41:(56):409-418.
14. Code of the Republic of Uzbekistan on Administrative Responsibility, Article 46. Retrieved from <https://lex.uz/docs/97661>; Criminal Code of the Republic of Uzbekistan, 1994, 141. Retrieved from <https://lex.uz/docs/111457>.
15. Council of Europe. Convention for the protection of individuals with regard to the processing of personal data Convention 108+. Retrieved from <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>; OECD. (2013). The OECD Privacy Framework. Retrieved, 2018. from [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf).