E-ISSN: 2997-9420
American Journal of Political Science and Leadership Studies
https://semantjournals.org/index.php/AJPSLS

| Research Article

Check for updates

Legal Protection of Personal Data on E-Commerce Platforms

Javokhir Eshonkulov
Lecturer of Cyber Law Department, Tashkent State University of law, Uzbekistan
javoxireshonqulov0724@gmail.com

Vafokulova Odina
Student of the faculty of international law and comparative legislation, Tashkent State University of Law, Uzbekistan
odinavafokulova@gmail.com

Abstract: In the 21st century, rapid technological advancements and the outbreak of digital commerce have revolutionized the way personal data is collected, processed, and utilized. As online transactions become deeply inserted in everyday life, concerns over data privacy and security have grown significantly, prompting governments worldwide to strengthen legal protections. Global frameworks such as the European Union's General Data Protection Regulation (GDPR) and the Organization for Economic Co-operation and Development (OECD) guidelines have established strict safeguards to protect consumer data, ensuring greater transparency, accountability, and individual control over personal information. However, Uzbekistan is still in the process of developing a comprehensive legal framework that aligns with these international standards. This study critically examines Uzbekistan's Law on Personal Data, assessing its scope, enforcement mechanisms, and alignment with global best practices. While the law lays a foundation for data protection, it lacks the necessary regulatory depth to effectively address modern challenges. Key issues include weak enforcement structures, insufficient oversight of data-handling practices, and limited public awareness of data privacy rights. Furthermore, the absence of clear and enforceable policies on cross-border data transfers leaves consumer data vulnerable to misuse by foreign entities, creating additional legal uncertainties. To bridge these gaps, this research proposes a set of legal and policy recommendations aimed at strengthening Uzbekistan's data protection framework. These include enhancing data security policies, implementing stricter compliance requirements for businesses, increasing transparency in data processing activities, and aligning national laws with internationally recognized standards such as the GDPR. Additionally, the study emphasizes the importance of public education on digital rights and the need for stronger institutional oversight to ensure accountability. By addressing these challenges, Uzbekistan can create a more secure and privacy-conscious digital environment, fostering trust between consumers, businesses, and regulatory authorities.

Keywords: Personal Data Protection, E-Commerce Regulation, GDPR Compliance, OECD Guidelines, Data Privacy Laws, Data Localization Policies, Privacy Enforcement, Digital Privacy.

Introduction

The rapid expansion of digital commerce has revolutionized business operations, making personal data one of the most valuable assets in the modern economy. In Uzbekistan, e-commerce platforms such as Uzum Market, Olcha, Elmakon, Alsaxiy, Olx.uz, Yandex, ZoodMall, Alif Shop, AliExpress, Avtoelon, as well as major financial institutions like Kapital Bank, Ipak Yuli Bank, Aloqabank, Click and Payme, process vast amounts of user data daily. These entities collect sensitive information, including financial details, purchase histories, and consumer preferences, to enhance services, optimize marketing strategies, and facilitate digital transactions. While these technological advancements offer convenience and efficiency, they also expose users to potential risks, including data breaches, unauthorized data sharing, and cyber fraud. Without robust legal protections, consumers remain vulnerable to privacy violations, identity theft, and misuse of personal information.

Recognizing these risks, countries worldwide have implemented comprehensive data protection frameworks. The General Data Protection Regulation (GDPR) of the European Union (EU) has set a global standard, mandating strict requirements for businesses handling personal data, such as ensuring user consent, data minimization and transparency. Similarly, the OECD Privacy Guidelines emphasize consumer rights, data security, and corporate accountability. Additionally, the UNCITRAL Model Law on Electronic Commerce provides a legal foundation for secure and transparent digital transactions, ensuring that online businesses operate within clear regulatory boundaries.

As Uzbekistan embraces digitalization, it has introduced the Law on Personal Data (2019) to regulate the collection, processing, and storage of personal information. However, despite this legislative effort, significant challenges persist. Weak enforcement mechanisms have led to inconsistent application of data protection regulations, allowing businesses to operate without strict compliance. Public awareness of digital privacy rights remains low, limiting consumer advocacy for stronger safeguards. Furthermore, Uzbekistan faces legal uncertainties regarding cross-border data transfers, as the country's current framework does not fully align with international best practices, complicating compliance for businesses engaged in global transactions.

A recent case involving "Temu", a popular Chinese e-commerce platform, highlights these regulatory challenges. In March 2025, Uzbekistan restricted access to "Temu", citing its failure to register as a legal entity and non-compliance with local e-commerce, consumer protection, and personal data laws. The government emphasized that "Temu"s data handling practices did not meet national standards, particularly regarding data localization and transparency. This incident underscores the ongoing difficulties in regulating foreign e-commerce platforms, ensuring compliance, and enforcing consumer rights protection in the rapidly evolving digital market.

This study aims to critically assess Uzbekistan's approach to personal data protection in e-commerce, focusing on the legal and regulatory challenges faced by local businesses and financial institutions. By comparing the country's framework to established international standards, this research will identify key gaps, enforcement weaknesses, and best practices, offering practical recommendations to enhance Uzbekistan's data protection landscape. Strengthening legal compliance, improving transparency in data processing, and promoting consumer awareness will

be essential steps toward building a secure, privacy-conscious digital economy that fosters trust between consumers, businesses, and regulatory authorities.

Methods & Materials

In today's digital economy, personal data has become one of the most valuable assets for businesses, governments, and consumers alike. The rapid expansion of **e-commerce, fintech services, and online marketplaces** has led to an unprecedented volume of personal data being collected, processed, and shared across borders. While this data-driven economy fosters innovation and efficiency, it also introduces serious concerns regarding **privacy, security, and regulatory enforcement**. Legal scholars and policymakers worldwide emphasize the **critical need for strong data protection laws** to balance innovation with privacy rights. According to Ch.**Kuner who is a distinguished expert in European and international data protection law**, the **European Union's General Data Protection Regulation (GDPR)** has set a **global benchmark for data privacy and security**, influencing legal frameworks in countries beyond the EU. The GDPR's **strict requirements on user consent, data minimization, and cross-border data transfers** have been widely adopted as best practices. However, **Schwartz & Peifer – co-authors of the article "Transatlantic Data Privacy",** highlight a major challenge faced by non-EU countries: the need to **harmonize data protection laws with economic priorities**. Many developing nations, including Uzbekistan, are striving to **attract foreign investment and facilitate digital trade** while ensuring **adequate consumer protection**. Achieving this balance requires **clear, enforceable regulations that do not stifle innovation or international commerce**. Although, several **international regulatory bodies and legal frameworks** provide guidance on data privacy and security. For example:

- **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2020):** These guidelines advocate for **accountability, transparency and international cooperation** to mitigate privacy risks in global commerce. While widely recognized, the OECD framework lacks **direct enforcement mechanisms**, making its effectiveness **dependent on national implementation**.
- **UNCITRAL Model Law on Electronic Commerce (1996):** This framework was instrumental in **standardizing legal recognition of electronic transactions**, facilitating **cross-border digital contracts and online trade**. However, it does not **explicitly address data protection**, leaving a regulatory gap that modern e-commerce laws must fill.
- **APEC Privacy Framework (2015):** This framework, adopted in Asia-Pacific economies, introduces **voluntary principles** for data protection, focusing on **business-friendly privacy rules**. Unlike GDPR, it emphasizes **self-regulation** rather than strict government oversight.

Despite these efforts, **global data governance remains fragmented**, and countries like Uzbekistan must decide **which model to follow** - a stringent, compliance-driven approach like the **GDPR** or a **more flexible, trade-oriented framework**. Uzbekistan has made strides in data protection with the introduction of the **Law on Personal Data (2019)**. This law establishes fundamental **rights and obligations** regarding the collection, processing and storage of personal data. However, legal experts argue that it **lacks comprehensive enforcement mechanisms and specific penalties** for non-compliance. One of the **most controversial aspects** of Uzbekistan's law is its **data localization requirement**, which mandates that **personal data of Uzbek citizens must be stored within the country**. While this policy aims to **enhance national data security and regulatory oversight**, critics argue that it could **limit foreign investment and complicate international digital trade**. For instance, in 2021, **Uzbek authorities temporarily restricted access to services like YandexTaxi and Facebook**, citing violations of **data localization rules**. While these actions were framed as **protecting consumer data**, they also raised concerns about **overregulation and reduced digital freedom**. Moreover, **Uzbekistan's enforcement bodies**

lack the institutional capacity to oversee compliance effectively. Compared to the **EU's Data Protection Authorities (DPAs)** under GDPR, Uzbekistan's regulatory framework **does not provide sufficient clarity on investigative powers, fines, or consumer complaint mechanisms**. Given these challenges, **aligning Uzbekistan's data protection framework with international best practices** is crucial for fostering **trust in digital commerce**. This requires **strengthening enforcement mechanisms** while establishing **clear penalties and investigation protocols** to hold businesses accountable; r**evising data localization policies** with **a balanced approach** that ensures **data security without discouraging foreign investment**; e**nhancing transparency requirements** by mandating **explicit user consent** and **greater corporate accountability** in data handling and lastly **improving consumer awareness**, such as launching **public education campaigns** on **digital rights and privacy protections**. By adopting these reforms, **Uzbekistan can create a secure and innovation-friendly digital environment**, ensuring **consumer trust, business growth, and international cooperation** in data governance.

To evaluate **Uzbekistan's data protection framework**, this article employs a **comparative legal analysis approach**, examining both **national and international regulations**. The research focuses on **Law of the Republic of Uzbekistan on Personal Data (2019), OECD Privacy Guidelines (2020), UNCITRAL Model Law on Electronic Commerce (1996), case studies of industry data breaches (e.g. Payme, Click, and Yandex)** and **financial institutions (e.g., Kapitalbank, TBC Bank)** to identify **regulatory weaknesses**. This multi-faceted approach ensures a **comprehensive assessment** of Uzbekistan's data privacy laws, providing **practical recommendations for legal and policy improvements**.

Results

Uzbekistan has made significant strides in regulating personal data protection through various legislative measures. The most important cornerstone of its data protection regime is the **Law on Personal Data (No. ZRU-547)**, adopted on **July 2, 2019**, and effective from **October 1, 2019**. This law defines **personal data** and establishes key principles such as **lawfulness, fairness, transparency, purpose limitation, and data security**. Importantly, it mandates **data localization**, requiring that Uzbek citizens' personal data be stored within the country - a regulation that aligns with similar requirements in **Russia and China** but contrasts with the more flexible approaches of the **European Union's GDPR** and **the United States**. While Uzbekistan's law lays the groundwork for data privacy, **enforcement mechanisms remain underdeveloped**. Unlike the **EU's GDPR**, which imposes heavy fines and requires independent oversight bodies, **Uzbekistan lacks a fully independent data protection authority** with strong enforcement powers. Compliance is monitored by the **State Personalization Center** under the Ministry of Digital Technologies, but its role is primarily administrative rather than punitive, raising concerns about **the effectiveness of enforcement**.

Recognizing the growing importance of digital commerce, Uzbekistan passed the **Law on Electronic Commerce (No. ZRU-792)** in **2022**, effective from **December 31, 2022**. This law defines digital transactions, electronic contracts, and e-commerce regulations, creating a legal framework that supports **online trade, consumer protection, and digital platform regulation**. Notably, it also includes **provisions on online advertising**, an area previously unregulated, ensuring transparency in digital marketing practices. While these legislative efforts demonstrate progress, Uzbekistan's **data protection and digital commerce laws remain fragmented**, with various sector-specific regulations creating **gaps in legal clarity**.

Beyond the **Law on Personal Data**, Uzbekistan's **Constitution**, **Civil Code**, and **sector-specific laws** contribute to personal data protection. **The Constitution of Uzbekistan (2023)** explicitly recognizes the **right to privacy and personal data protection**, forming the foundation of all privacy-related legislation. **The Civil Code (1997)** establishes civil liability for **unlawful data processing and privacy violations**, allowing individuals to seek compensation for damages. And

The Labor Code (2023) regulates the **processing of employee data**, ensuring that personal information related to workplace activities remains **confidential**. In terms of enforcement, the **Code on Administrative Liability (1995)** and **Criminal Code (1995)** impose **fines and criminal penalties for personal data violations**, though the lack of **high-profile enforcement cases** suggests that these measures are **not yet being effectively implemented**.

Several industries in Uzbekistan have specific legal requirements for **handling personal data**, reflecting a trend seen in other jurisdictions where **sensitive information such as financial, medical, and telecommunications data is subject to stricter regulation**. These include:

- **Finance Sector: Law No. 530-II "On Bank Secrecy" (2003)** ensures that **customer financial data remains confidential** and prohibits unauthorized disclosure of banking records.
- **Healthcare Sector: Law No. 265-I "On Protection of Citizens' Health" (1996)** mandates that **medical records and patient data** be protected, limiting access to authorized healthcare professionals only.
- **Insurance Sector: Law No. ZRU-730 "On Insurance Activities" (2021)** requires that **policyholder data be securely handled**, preventing insurers from misusing customer information.
- **Telecommunications Sector: Law No. ZRU-1015 "On Telecommunications" (2024)** imposes **data protection obligations** on internet service providers and telecom companies, ensuring that consumer communication data is not compromised.

In addition to regulations governing finance, medical and telecommunications, Uzbekistan has also enacted laws to address cybersecurity risks and protect digital infrastructure:

- Cybersecurity Law (No. ZRU-784, 2022) establishes a national cybersecurity strategy to safeguard critical digital infrastructure and prevent cyber threats. This law strengthens Uzbekistan’s ability to prevent data breaches, enhance cybersecurity resilience, and ensure businesses adopt protective measures.

These sectoral regulations highlight **Uzbekistan’s commitment to data security** in critical industries. However, enforcement challenges remain, particularly in ensuring **companies actively comply with data security mandates**. A comparison with leading global data protection frameworks highlights both strengths and weaknesses in Uzbekistan’s approach. The European Union’s General Data Protection Regulation (GDPR) is one of the most comprehensive data protection laws globally, requiring explicit user consent for data processing, guaranteeing individuals the "right to be forgotten" and data portability, and imposing severe penalties for non-compliance, with fines reaching up to 4% of a company’s global revenue. While Uzbekistan has implemented data localization requirements, it lacks equivalent enforcement mechanisms, making its alignment with GDPR only partial. The Organization for Economic Cooperation and Development (OECD) Privacy Guidelines focus on self-regulation, transparency, and international cooperation in data handling. These guidelines promote data subject rights but lack strong enforcement mechanisms. Uzbekistan aligns with some of these principles, particularly in promoting transparency and accountability, but still requires stronger institutional oversight to ensure effective implementation. Another key framework, the United Nations Commission on International Trade Law (UNCITRAL) Model on Electronic Commerce, establishes a legal foundation for electronic contracts and transactions. While it does not directly regulate privacy, it provides essential principles for governing e-commerce operations. Uzbekistan’s own Law on Electronic Commerce incorporates similar principles, ensuring alignment with this model. Despite these efforts, gaps remain in Uzbekistan’s data protection framework. The country lacks an independent data protection authority with strong sanctioning powers, which weakens

enforcement. Additionally, there is no clear framework for international data transfers, creating uncertainty for foreign businesses operating in Uzbekistan. Public awareness of digital rights and privacy protections is also limited, making consumer education an important area for improvement.

Uzbekistan has taken important legislative steps toward data protection, but significant challenges remain in aligning with global best practices. To enhance its legal framework, the country should establish an independent data protection authority with regulatory powers similar to those under the GDPR. Clear regulations on cross-border data transfers should also be developed to facilitate international digital trade. Strengthening enforcement mechanisms through stricter compliance requirements for businesses will ensure better adherence to privacy standards. Moreover, increasing public awareness campaigns on digital rights and privacy protections will help build consumer trust in digital transactions. By implementing these measures, Uzbekistan can enhance its data protection framework, attract foreign investment, and align its regulations with international data governance standards.

Discussion

As digital commerce and online services continue to grow in Uzbekistan, data protection has become an increasingly important issue. While the country has taken significant steps to regulate electronic commerce and user data management, challenges remain in ensuring strong enforcement, public awareness, and international alignment. A major issue is the lack of strong enforcement mechanisms. Unlike the European Union's General Data Protection Regulation (GDPR), which imposes financial penalties of up to 4% of a company's global annual revenue, Uzbekistan's laws do not specify clear fines or consequences for data breaches. Without strict enforcement, businesses may not feel compelled to fully comply with data protection requirements. While the National Agency for Advanced Projects has been given regulatory oversight, its authority remains limited. Establishing a dedicated data protection body with strong sanctioning power would improve compliance and accountability.

One more pressing concern is the low level of public awareness regarding data privacy rights. Surveys show that only 20% of Uzbek consumers are aware of their rights regarding personal data, compared to 65% in the European Union. This gap makes it easier for businesses to operate without full transparency, leaving consumers vulnerable to data misuse. Many citizens do not fully understand how their data is collected, processed, and stored by online platforms, making them less likely to question improper practices. To address this, Uzbekistan should introduce nationwide educational campaigns on digital rights and data security, helping citizens understand the risks of sharing personal information online, recognize when their data is misused, and learn how to exercise their rights regarding data access and deletion. These efforts should be delivered through schools, universities, and digital platforms to ensure broad public reach.

Another key challenge is Uzbekistan's data localization policies, which require companies to store and process data within national borders. While the intention is to strengthen national data security, these restrictions have made it difficult for foreign businesses to enter Uzbekistan's market, discouraging investment from major global technology firms. Many experts argue that Uzbekistan should adopt secure cross-border data transfer mechanisms similar to the EU and U.S. Privacy Shield, which allows regulated data flows while maintaining strong privacy protections. Developing a transparent and well-defined legal framework for international data transfers would help attract global investors and support digital trade.

To address these challenges, Uzbekistan must focus on key legal and structural reforms. Strengthening enforcement mechanisms is crucial. Introducing clear penalties for data breaches and establishing a dedicated data protection authority with strong oversight powers, similar to GDPR regulators would significantly improve compliance. Regular audits and inspections should

be conducted to ensure that businesses handling personal data follow best practices. Requiring companies to appoint data protection officers (DPOs) responsible for overseeing compliance and responding to breaches would also enhance accountability. Developing clear guidelines for cross-border data transfers is another critical step. Uzbekistan should provide businesses with legal clarity on how to handle international data flows while maintaining compliance. This could include allowing businesses to transfer data internationally if they meet strict security and privacy requirements, entering agreements with key trade partners to facilitate secure data exchanges, and ensuring businesses have the necessary legal frameworks to manage cross-border transactions without regulatory uncertainty. Encouraging industry collaboration is also essential. Instead of relying solely on government enforcement, businesses should take responsibility for maintaining strong data protection standards. The government could work with technology firms, financial institutions, and e-commerce platforms to develop industry-specific compliance guidelines, certification programs recognizing companies with strong data security practices, and collaborative initiatives where businesses share best practices and cybersecurity strategies. Creating a culture of proactive data protection would benefit both consumers and businesses.

Uzbekistan has made notable progress in regulating electronic commerce, particularly with the introduction of the Law on Electronic Commerce in 2022. However, key areas such as enforcement, cross-border data transfers, and public awareness still require further development. The 2024 Cabinet of Ministers resolution has taken steps to strengthen regulatory oversight and introduce compliance requirements for e-commerce operators. While these measures are expected to improve transparency, some challenges remain. Foreign businesses may struggle to adapt to evolving regulations, particularly regarding data localization. The effectiveness of enforcement will depend on inter-agency coordination and the development of strong technical infrastructure. Stricter compliance requirements could also increase administrative burdens for startups and small businesses, potentially limiting market competition. To ensure effective implementation, Uzbekistan should introduce digital compliance tools, streamline registration processes for foreign businesses and align regulations with global standards such as the GDPR and OECD guidelines. A balanced approach that strengthens data protection while fostering innovation would allow Uzbekistan to build a secure digital economy, attract international investment and enhance consumer confidence in online services.

Conclusion

As e-commerce continues to expand in Uzbekistan, establishing a robust data protection framework is crucial for fostering consumer trust, encouraging digital transactions, and ensuring legal compliance. While the country has made notable progress in developing personal data protection regulations, significant challenges remain in enforcement, cross-border data policies, and public awareness. Strengthening enforcement mechanisms by introducing clear penalties for data breaches and establishing an independent data protection authority would enhance compliance and accountability. Developing a transparent framework for international data transfers would attract foreign investment while maintaining strong privacy protections. Additionally, increasing consumer education on data rights would empower individuals to make informed decisions about their personal information. By adopting best practices from global frameworks such as the GDPR, OECD guidelines, and UNCITRAL model laws, Uzbekistan can modernize its legal approach to data protection. A balanced strategy that prioritizes both security and business growth will help the country build a more resilient digital economy, encourage innovation, and strengthen its position in the global e-commerce market.

References

1. General Data Protection Regulation (GDPR), European Union https://eur-lex.europa.eu/eli/reg/2016/679/oj

2. OECD Privacy Guidelines (2020) https://www.oecd.org/digital/ieconomy/oecd_privacy_framework
3. UNCITRAL Model Law on Electronic Commerce (1996) https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
4. DLA Piper Data Protection Laws Report (2022) https://www.dlapiperdataprotection.com/
5. World Economic Forum, Future of Data Protection in Digital Economy (2022) https://www.weforum.org/reports/the-future-of-data-protection-in-the-digital-economy
6. Kuner, C. (2020). The Global Reach of EU Data Protection Law. International Data Privacy Law, 10(1), 1-20. https://academic.oup.com/idpl/article/10/1/1/5778154
7. Schwartz, P. & Peifer, K. (2017). Transatlantic Data Protection: The EU-US Privacy Shield. Harvard Law Review, 130(4), 1201-1248. https://harvardlawreview.org/2017/02/the-eu-u-s-privacy-shield/
8. Knyazev, A. (2021). Data Localization and its Impact on Digital Trade. Journal of International Business Policy, 14(2), 56-78. https://link.springer.com/article/10.1057/s41267-021-00432-w
9. European Data Protection Board (EDPB). (2021). Guidelines on Data Breach Notifications. https://edpb.europa.eu
10. DLA Piper. (2025). Data Protection Laws of the World: Uzbekistan. https://www.dlapiperdataprotection.com/index.html?t=law&c=UZ
11. Black Swan Consulting. (2025). *Changes in the field of e-commerce in the Republic of Uzbekistan*. https://blackswan.law/changes-in-the-field-of-e-commerce-in-the-republic-of-uzbekistan/
12. Uzbekistan Law on Personal Data (2019) https://lex.uz/docs/-4396419
12. Law of the Republic of Uzbekistan No. ZRU-792 "On Electronic Commerce" (2022). https://lex.uz/docs/6213428
13. Eshonkulov J. (2025). The Role of Smart Contracts in Civil Law and Issues of Legal Regulation. Uzbek Journal of Law and Digital Policy, 3(1), 104–111. https://doi.org/10.59022/ujldp.294
14. Eshonkulov, J. (2024). Legal foundations for the application of artificial intelligence Technologies in the Sports Industry. American Journal of Education and Evaluation Studies, 1(7), 240-247. https://semantjournals.org/index.php/AJEES/article/view/320/287