DATA LOCALIZATION REQUIREMENT

Kamarova Zarina Behzod kizi
Graduate student at the University of World Economy and Diplomacy,
100007, Republic of Uzbekistan, Tashkent, Mustakillik ave., 54
e-mail: zarinakamarova787@gmail.com

Annotation. *This article explores the importance of personal data protection regulation in Uzbekistan and its impact on international business, trade, and e-commerce in the country. It highlights the significant changes brought about by the Personal Data Protection Act, focusing on its influence on data transfer, cross-border business operations, consumer trust, and competitiveness in the global market. The article concludes with recommendations for businesses operating or seeking to expand into Uzbekistan to ensure compliance and build a strong foundation for success in the evolving digital era.*

Key words: *Data Protection, Personal Data Protection Regulation, Data Localization, Uzbekistan, International Business, Trade, E-commerce, Data Transfer, Cross border Data Transfer, Competitiveness, Consumer Trust.*

Personal data protection has become an increasingly critical concern for nations worldwide. In Uzbekistan, the enforcement of the Personal Data Protection Act has paved the way for new requirements and guidelines aimed at safeguarding individuals' personal information. This article aims to explore the impact of personal data protection regulation on international business, trade, and e-commerce in Uzbekistan.

The official website of the United Nations Conference on Trade and Development (UNCTAD) has published a list of governments that have enacted laws to protect personal data. As more social and commercial activity move online, the necessity of privacy and data security is becoming more widely understood. Equally concerning is the acquisition, use, and disclosure of personal information to other parties without consumer notification or consent. 137 of 194 nations had enacted legislation to provide data and privacy protection. Africa and Asia have varied levels of acceptance, with 61 and 57% of nations adopting such laws, respectively. The least developed countries account for only 48% of the total. Furthermore, while 9 percent of states are in the process of drafting legislation to safeguard personal data (draft legislation), the remaining 15% are governments that have no data protection legislation at all. These figures illustrate that the protection of personal data, the development of a legal

framework for it, and the enhancement of secrecy are becoming increasingly crucial across the world.

Due to the importance of regulating personal data interconnections in Uzbekistan, the Law on Personal Data was enacted in 2019. It is demonstrated that the new Law applies to all relationships that arise, independent of the processing tools, including information technology, utilized in the transmission and preservation of information.

Apart from the Law on Personal Data, there are certain legal acts that establish fundamental principles of data protection processing and / or set liability for violation of data protection rules. They include:

- Constitution of the Republic of Uzbekistan entered into force on December 8, 1992.
- Civil Code of the Republic of Uzbekistan entered into force on 1 March 1997.
- Labor Code of the Republic of Uzbekistan entered into force on 1 April 1996.
- Code of the Republic of Uzbekistan on Administrative Liability entered into force on 1 April 1995 (‘Code on Administrative Liability’).
- Criminal Code of the Republic of Uzbekistan entered into force 1 April 1995 (‘Criminal Code’).
- Law No. 439-II 'On Principles and Guarantees of Freedom of Information' dated December 12, 2002; and
- Law No. 560-II 'On Informatization' dated December 11, 2003.

Article 27-1 was added to the legislation on the basis of the statute issued on the initiative of the State Center for Personalization under the Cabinet of Ministers on January 14, 2021, with the following content:

“Owner and (or) operator in the processing of personal data of citizens of the Republic of Uzbekistan using information technology, including the processing of the Internet in the global information network, their physical means located in the territory of the Republic of Uzbekistan and in the prescribed manner must ensure the collection, systematization and storage of databases in the databases of the person registered in the state register”.

What does the adoption of a new standard represent?

Article 27-1 requires social networks and Internet services to keep the personal data of Uzbek individuals on servers located in Uzbekistan. In other words, Facebook, Google, Telegram, and other services demand the storage of personal data of Uzbek individuals on Uzbek territory. There is also a perspective that the implementation of

this standard is nothing more than a restriction on free expression and opinion in society, and this blog article will address this topic and present a valid conclusion.

It should be highlighted that the inclusion of Article 27-1 in legislation and the execution of this regulation demonstrate that the government has constructed massive data centers on its territory to store information about Internet users as well as the public. Personal information will be stored in these databases, which may be seen in a number of countries, including the Russian Federation, China, and Scandinavian countries.

Facebook has complained that holding personal information within the state is bad for the economy and human rights, and that data localization throughout the world poses a substantial risk to users' privacy, freedom of expression, security, and human rights. Before enacting the article, the government stated that it had examined the experiences of a number of foreign nations, including the United States, Europe, Australia, India, Kazakhstan, Indonesia, and Turkey. The inclusion of this clause in the Act was explained by government officials as follows: the government cannot monitor compliance with legal obligations. Even if Uzbek enterprises keep personal information in another nation, the government cannot supervise how the regulations are implemented because it lacks the power to conduct inspections in that country.

Furthermore, "Facebook Inc." (Facebook Messenger, Instagram, WhatsApp), Google (Google Messenger, YouTube), Mail.ru (Vkontakte, Odnoklassniki), Microsoft (Skype), Telegram, Tencent (Wechat), TikTok, Twitter, Yandex -emails were sent to ensure the collection and storage of personal data of Uzbek citizens on technical devices located in Uzbekistan. To assure the new law's application, the Cabinet of Ministers passed Resolution No. 255, which included the Statute as an annex.

First, it will be discussed what data localization is? Data localization is the practice of preserving data inside the location from where it originated. For example, if a company gathers data in the UK, it will keep it there rather than sending it to another nation for processing. Because the Internet allows data to go around the world in milliseconds, regulators, privacy activists, and consumers are becoming increasingly interested in where that data travels and what is done with it.

First of all, data localization assists in the storage and privacy protection of personal data. Specifically, on September 1, 2015, the Law FZ-242 regulations went into effect in the Russian Federation (Russia). This implies that Russian personal data operators handle and store their data using databases that are situated within Russia. Stated differently, it is evident that foreign corporations want to keep track of personal information in sizable data centers situated within Russian territory. Furthermore, the

operations of data centers are outlined in the Regulation "On the localization of certain processes of storage and processing of personal data" in Russia.

Russia benefits economically from data localization, which may also open up new opportunities for the IT sector to expand. The building of data processing centers (DPC) that provide location and cloud services, in particular, will be a new driver of growth for the Russian IT sector. The Russian data center market is expected to expand by 27% annually in 2019. According to a recent analysis by market research firm iKS-Consulting, sib is $561 million. The market for cloud services and data centers in Russia is performing well, according to the report, with growth rates for location services and cloud services approaching 25% and 10%, respectively. Additionally, the data revealed that there were 43.5 thousand shelves, an increase of 11%.

Data localization has drawbacks as well, as the following examples show:

The nationwide distribution of data centers can lead to many obstacles and challenges for e-commerce, as well as restricted options for buyers. What say you, sir? Online sales of products and services are becoming more and more significant for worldwide business in the current technological era. Based on statistical data, the amount of money sold online in the US in 2019 was close to $150 billion, or 11% of total retail sales. In a similar vein, goods commerce accounts for 12% of global trade online. Data localization has an impact on commerce, but it also runs the danger of stifling innovation and obstructing the technical benefits of unrestricted data flow. These regulations have the potential to impede the free and open Internet, tax new entrants, and erect obstacles that restrict consumer choice, all of which can negatively impact the Internet and data flow. In other industries, like the banking sector, they might be very noticeable. Furthermore, American technology firms and non-technological enterprises that utilize data face extra obstacles as a result of the European approach, which includes the General Regulation on Data Protection (GDPR) and localization requirements. Protectionist obstacles that raise operating costs and lessen the advantages of cross-border flows have been established in the nation or area as a consequence, which is also making it difficult for the number of people to travel abroad.

It is challenging for new goods and services to expand internationally due of data localization. This is due to the fact that small and medium-sized enterprises looking to enter a new market incur higher expenses as a result of the criteria for local availability or preservation of local content. For instance, research by Leviathan Security Group discovered that the cost of data deployment is increased by 30–60% due to data localization requirements.

Storing data centers in the country creates a number of barriers and difficulties in online international trading of Uzbekistan.

Data Localization Requirements: Some countries impose data localization requirements, mandating that certain types of data related to citizens or consumers must be stored within the country's borders. This can create barriers for international companies engaged in online trading, as they are required to establish and maintain local data centers to comply with these regulations. For example, in Russia, regulatory measures such as the Data Localization Law have required companies to store Russian citizens' personal data on servers located within the country, posing challenges for international e-commerce platforms and service providers.

Increased Operational Costs: Building and maintaining data centers can significantly increase operational costs for online trading businesses. Establishing and managing local data centers typically require substantial investments in infrastructure, security, and compliance with local regulations. These costs can strain the resources of international businesses operating in the country, potentially impacting their competitiveness and profitability.

Complexity in Managing Data Compliance: Operating data centers in a specific country entails adherence to local data protection laws and regulations. International businesses must navigate different legal frameworks, leading to complexities in ensuring compliance with varying data protection requirements. For example, in the European Union, the General Data Protection Regulation (GDPR) places stringent requirements on how personal data is handled, creating challenges for non-EU businesses storing and processing data within the region.

Data Security and Resilience Concerns: Geopolitical and local business environment factors can impact the security and resilience of data stored within a specific country. For instance, in regions prone to political instability or frequent power outages, maintaining consistent data accessibility and security becomes challenging. This can pose risks for online trading operations, particularly in ensuring seamless and secure transactions for international clientele.

Limited Flexibility in IT Infrastructure Deployment: Requiring data storage within a specific country limits the flexibility of international businesses to deploy and manage their IT infrastructure in a manner that optimally supports their global trading operations. Businesses may face barriers in leveraging cloud-based services and global content delivery networks to efficiently serve their international customer base due to the restricted data storage mandates.

These examples highlight the multifaceted challenges that storing data centers in a specific country can pose for international online trading. While data localization aims to address certain policy goals, it is essential to balance these factors with the overarching aim of fostering a conducive environment for international e-commerce and digital trade.

This article encapsulates the growing importance of personal data protection regulation in Uzbekistan within the context of international business, trade, and e-commerce, reflecting both the challenges and the opportunities that lie ahead for businesses and regulators in the country. The enforcement of personal data protection regulation in Uzbekistan has ushered in transformative changes for international business, trade, and e-commerce sectors in the country. Compliance with data protection regulations ensures seamless data transfer, enhances consumer trust, and strengthens competitiveness in the global market. Businesses operating or seeking to expand into Uzbekistan must adopt and adhere to proper personal data protection practices to position themselves for success in today's digitally driven business landscape.

Bibliography

Boardman R, *DATA PROTECTION STRATEGY: Implementing Data Protection Compliance*. (2018)

Czinkota MR, Ronkainen IA and Moffett MH, *International Business* (Wiley 2021)

Greenleaf G, 'Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018' [2018] SSRN Electronic Journal

Mattoo A and Meltzer JP, 'International Data Flows and Privacy: The Conflict and Its Resolution' (2018) 21 Journal of International Economic Law 769

Serge Gijrath and others, *Concise European Data Protection, E-Commerce and IT Law* (Kluwer Law International BV 2018)

LAW OF THE REPUBLIC OF UZBEKISTAN ABOUT PERSONAL DATA 2019

LAW OF THE REPUBLIC OF UZBEKISTAN ON AMENDMENTS AND ADDITIONS TO SOME LEGISLATIVE ACTS OF THE REPUBLIC OF UZBEKISTAN 2020