A COMPARATIVE LEGAL ANALYSIS OF THE ROLE OF STATE BODIES AND LEGAL PROBLEMS IN ENSURING THE SECURITY OF PERSONAL DATA ON DIGITAL PLATFORMS

Davronov Otabek Bakhtiyor ugli
PhD Candidate at Tashkent State University of Law
https://doi.org/10.5281/zenodo.21186795

ANNOTATSIYA

Ushbu maqolada raqamli platformalar sharoitida shaxsga doir ma'lumotlar xavfsizligini ta'minlashda davlat organlarining o'rni qiyosiy-huquqiy nuqtai nazardan tahlil qilinadi. Tadqiqot O'zbekiston Respublikasi Kiberxavfsizlik markazi davlat muassasasida o'talgan ilmiy stajirovka davomida to'plangan materiallar, amaliy kuzatuvlar, normativ-huquqiy hujjatlar tahlili, xorijiy tajriba hamda ilmiy manbalarni o'rganish natijalariga asoslanadi. Tadqiqot doirasida O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni, Kiberxavfsizlik markazi hamda Shaxsiylashtirish agentligining shaxsga doir ma'lumotlarni himoya qilish sohasidagi vakolatlari Yevropa Ittifoqining Umumiy ma'lumotlarni himoya qilish reglamenti (GDPR) hamda Janubiy Koreyaning Shaxsiy ma'lumotlarni himoya qilish komissiyasi (PIPC) tajribasi bilan qiyosiy-huquqiy jihatdan tahlil qilinadi. Maqola yakunida milliy qonunchilikni va institutsional mexanizmlarni takomillashtirishga qaratilgan ilmiy asoslangan taklif va tavsiyalar ilgari suriladi.

Kalit so'zlar: shaxsga doir ma'lumotlar, raqamli platformalar, kiberxavfsizlik, ma'lumotlarni himoya qilish agentligi, GDPR, qiyosiy huquq, institutsional mustaqillik.

АННОТАЦИЯ

В данной статье с позиции сравнительно-правового анализа исследуется роль государственных органов в обеспечении безопасности персональных данных в условиях функционирования цифровых платформ. Исследование основано на материалах, собранных в ходе научной стажировки в Государственном учреждении «Центр кибербезопасности» Республики Узбекистан, включая результаты практических наблюдений, анализ нормативно-правовых актов, изучение зарубежного опыта и научной литературы. В рамках исследования проводится сравнительно-правовой анализ Закона Республики Узбекистан «О персональных данных», полномочий Центра кибербезопасности и Агентства персонализации в сфере защиты персональных данных с положениями Общего регламента Европейского союза по защите данных (GDPR), а также опытом Комиссии по защите персональной информации Республики Корея (PIPC). В заключение статьи сформулированы научно обоснованные предложения и рекомендации, направленные на совершенствование национального законодательства и институциональных механизмов защиты персональных данных.

Ключевые слова: персональные данные, цифровые платформы, кибербезопасность, орган по защите данных, GDPR, сравнительное право, институциональная независимость.

ABSTRACT

This article provides a comparative legal analysis of the role of public authorities in ensuring the security of personal data on digital platforms. The research is based on materials collected during a scientific internship at the Cybersecurity Center of the Republic

of Uzbekistan, including practical observations, an analysis of legal and regulatory documents, foreign experience, and relevant academic literature. The study examines the Law of the Republic of Uzbekistan "On Personal Data", as well as the powers of the Cybersecurity Center and the Personalization Agency in the field of personal data protection, comparing them with the European Union's General Data Protection Regulation (GDPR) and the experience of the Personal Information Protection Commission (PIPC) of the Republic of Korea. The article concludes with scientifically grounded proposals and recommendations aimed at improving national legislation and institutional mechanisms for the protection of personal data.

Keywords: personal data, digital platforms, cybersecurity, data protection authority, GDPR, comparative law, institutional independence.

1. INTRODUCTION

The rapid expansion of digital platforms — e-commerce marketplaces, mobile banking applications, ride-hailing services, social networks, and public e-government portals — has turned personal data into one of the most valuable and most vulnerable assets of the modern economy. Every transaction on such a platform generates identifiers, biometric traces, behavioral patterns, and financial records that, if mishandled, expose individuals to fraud, discrimination, and loss of autonomy over their private life. For a rapidly digitalizing economy such as Uzbekistan, where the number of internet and mobile-application users has grown sharply over the past decade, the question of who guards this data, and with what legal tools, is no longer a purely technical matter but a constitutional one, directly connected to the right to privacy guaranteed by the Constitution.

The legal foundation for personal-data processing in Uzbekistan is the Law “On Personal Data” No. ZRU-547 of 2 July 2019, which was subsequently reinforced by localization requirements, a state registry of personal-data bases, and, most recently, sector-specific breach-notification duties for the financial sector introduced in 2025[1]. At the same time, day-to-day technical protection of information systems, incident response, and website security audits are entrusted to a separate institution — the Cybersecurity Center, a state institution operating under the Ministry for Digital Technologies[2]. This institutional split between a data-protection regulator and a cybersecurity operator is not unique to Uzbekistan; it mirrors, with important differences, the architecture found in the European Union and in the Republic of Korea.

The purpose of this article is to conduct a comparative-legal analysis of how state bodies in Uzbekistan, the European Union, and the Republic of Korea are organized to protect personal data on digital platforms, to identify the legal problems that arise from this organization — particularly gaps in institutional independence, enforcement power, and inter-agency coordination — and to formulate recommendations for improving Uzbekistan's regulatory framework in light of recent legislative developments and recorded security incidents.

2. RESEARCH METHODOLOGY

The research relies on the comparative-legal method as its principal tool, examining three jurisdictions selected for their contrasting institutional models: Uzbekistan (a centralized, executive-branch model in transition), the European Union (a fully independent supervisory-authority model under the GDPR), and the Republic of Korea (a model that evolved from an advisory body into an independent central administrative agency, the PIPC).

[1]Constitution of the Republic of Uzbekistan (new edition, effective 1 May 2023), Article 27.
[2]Law of the Republic of Uzbekistan "On Personal Data" No. ZRU-547, dated 2 July 2019, effective 1 October 2019.

This selection allows the study to trace a spectrum of institutional independence and to test which features correlate with more effective enforcement.

In addition to the comparative method, the article applies the formal-legal (dogmatic) method to interpret the text of the Law “On Personal Data” and related by-laws, and the systemic method to examine how this law interacts with the Law “On Cybersecurity,” the Law “On Informatization,” and sector-specific acts on e-commerce and telecommunications. A case-study approach is used with respect to two recent, publicly reported incidents involving Uzbek state information systems, which serve as empirical illustrations of the practical consequences of the current institutional arrangement. Sources include primary legislation, official statements of the Cybersecurity Center, and secondary analytical materials published by international legal-compliance platforms during 2025–2026.

3. RESEARCH RESULTS

3.1. Institutional architecture in Uzbekistan

Uzbekistan’s personal-data regime is anchored in the Law “On Personal Data”[3], which defines data subjects’ rights, sets registration obligations for databases with the State Register of Personal Data Bases, and imposes a general duty to store certain categories of citizens' data on servers located within the country[4]. Supervisory functions over this registry have historically been distributed between the Personalization Agency and the Ministry of Justice, while the Cybersecurity Center focuses on technical protection: auditing information-security compliance of websites in the national ".uz" domain, certifying information-security management systems, and coordinating incident response through UZCERT[5]. This means that a data breach on a digital platform in Uzbekistan can trigger the involvement of at least three distinct bodies — the data-protection registrar, the cybersecurity operator, and, for regulated sectors such as banking, the sectoral regulator — without a single agency bearing final, GDPR-style enforcement responsibility.

Recent reforms show two, partly opposite, trends. On one hand, Presidential Decree No. PP-153 of 30 April 2025 introduced compulsory breach notification and legal liability for data incidents in the financial sector, signaling a shift toward practical accountability. On the other hand, amendments signed on 26 March 2026 relaxed the strict data-localization requirement, permitting storage of most categories of personal data on foreign servers where the destination country is recognized as offering adequate protection, or where standard contractual clauses, binding corporate rules, or approved international standards are applied — while biometric, genetic, and telecom-subscriber data must still be stored domestically[6]. This liberalization was explicitly motivated by the need to accommodate international payment platforms such as PayPal, Apple Pay, and Google Pay, illustrating how digital-platform economics can reshape data-protection policy.

3.2. The European Union model

Under the GDPR, each member state must establish one or more independent public supervisory authorities responsible for monitoring compliance and protecting the fundamental rights of individuals[7]. These Data Protection Authorities possess investigative, corrective, and authorization powers, including the ability to impose administrative fines of

[3]Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 71, dated 8 February 2020, "On Approval of the Regulation on the State Register of Personal Data Bases."
[4]Freedom House, "Uzbekistan: Freedom on the Net 2024" — on the 2021 amendments obliging localization of data storage and registration of servers with Uzkomnazorat.
[5]Legal500, "Personal Data Compliance in Uzbekistan" (2025) — on Presidential Decree No. PP-153 of 30 April 2025 introducing breach-notification duties for the financial sector.
[6]The Times of Central Asia, "Uzbekistan Eases Data Localization Rules to Support Global Payment Platforms," February 2026.
[7]DLA Piper, "Data Protection Laws of the World Handbook," Uzbekistan chapter (2025 edition) — on the Personalization Agency's supervisory and registry functions.

up to EUR 20 million or 4% of an undertaking's global annual turnover, whichever is higher[8]. Cross-border cases are managed through a “one-stop-shop” mechanism coordinated by the European Data Protection Board, which prevents conflicting rulings across jurisdictions and gives platforms operating in multiple states a single lead authority to deal with. The defining feature of this model is not merely the existence of a regulator, but its formal independence from the executive branch and its concentration of both investigative and punitive power in one body.

3.3. The Republic of Korea model

South Korea’s Personal Information Protection Commission (PIPC) offers an instructive evolutionary example. When first created in 2011, the PIPC was merely an advisory panel attached to the Ministry of the Interior and Safety. Only after the 2020 amendment of the Personal Information Protection Act did it become a fully independent central administrative agency, equal in status to a government ministry, with power to investigate, adjudicate disputes, and sanction violators directly[9]. The practical effect of this independence became visible in 2025, when the PIPC imposed a penalty of approximately KRW 134.7 billion (about USD 93 million) on a major telecommunications carrier after a breach affecting roughly 23 million users, alongside parallel investigations into e-commerce and financial-sector breaches affecting tens of millions of additional records[10]. In the same period, the PIPC issued its first adequacy decision recognizing the EU as offering comparable protection, illustrating how a strong domestic enforcement record can translate into international regulatory trust and easier cross-border data flows[11]. The PIPC’s 2025 policy agenda additionally shows a shift toward proactive, risk-based inspection of high-risk platforms rather than purely reactive, complaint-driven enforcement.

3.4. Comparative findings and identified legal problems

Three structural problems emerge from this comparison. First, Uzbekistan's institutional model still distributes data-protection and cybersecurity functions across several bodies without a single authority holding both investigative and sanctioning power comparable to the EU’s Data Protection Authorities or Korea's PIPC; this fragmentation risks slow, uncoordinated responses to incidents involving digital platforms that combine payment, communication, and identity data in a single ecosystem.

Second, the practical cost of this gap is not hypothetical. In February 2026, media reports alleged that personal data belonging to at least fifteen million Uzbek citizens had been leaked from government systems and offered for sale on the dark web; two months later, a hacker separately claimed to possess and threatened to publish personal data of about one hundred employees of the Cybersecurity Center itself, a claim the Center denied while confirming that an internal investigation was under way[12]. Whatever the ultimate factual findings in these cases, the sequence — a large-scale allegation, an official rebuttal, and a further incident implicating the very body responsible for cybersecurity oversight — illustrates the reputational and systemic risk created when no single, sufficiently empowered and clearly accountable authority is publicly recognized as the guarantor of personal-data security.

[8]Kiberxavfsizlik markazi (Cybersecurity Center of the Republic of Uzbekistan), official service description, csec.uz — website and information-system security audits, incident response.
[9]Regulation (EU) 2016/679 (General Data Protection Regulation), Article 51.
[10]GDPR, Article 83 — administrative fines of up to EUR 20 million or 4% of annual global turnover, whichever is higher.
[11]GDPR-EU.org, "Who Is Responsible for Enforcing the GDPR?" — on the one-stop-shop mechanism and the European Data Protection Board.
[12]Chambers and Partners, “Data Protection & Privacy 2026 — South Korea,” Global Practice Guides — on the KRW 134.7 billion penalty imposed on SK Telecom following a breach affecting approximately 23 million users, and on breaches at Coupang and LotteCard.

Third, sanction levels remain comparatively underdeveloped. Neither the Law "On Personal Data" nor related acts on e-commerce and telecommunications[13] provide for turnover-based administrative fines of the kind used under the GDPR or the PIPA; liability instead relies mainly on the Code on Administrative Liability and, in serious cases, the Criminal Code, which were not drafted with large-scale platform breaches in mind. Without a credible, proportionate sanctioning mechanism tied specifically to data-protection violations, compliance incentives for large digital platforms remain weak.

4. RECOMMENDATIONS

4.1. Consolidate and formally strengthen institutional independence

Uzbekistan should consider consolidating personal-data supervision — currently split between the Personalization Agency's registry function and the Cybersecurity Center's technical function — into a single authority with a clearly defined statutory mandate covering both compliance oversight and incident investigation, following the trajectory the Republic of Korea followed when it transformed the PIPC from an advisory panel into an independent central administrative agency in 2020. Formal independence from ordinary line-ministry control, secure funding, and a fixed-term, removable-for-cause leadership would increase public trust and reduce the appearance of conflict of interest when the same institution investigates incidents involving government systems, as occurred with the Cybersecurity Center in 2026.

4.2. Introduce proportionate, turnover-based sanctions

The current administrative-liability regime should be supplemented with a graduated fine structure calibrated to the severity of the violation and, for major platform operators, to annual turnover, similar in principle to the GDPR's two-tier fine system. Such a mechanism should be paired with clear procedural safeguards — the right to be heard, a defined investigation timeline, and a judicial-appeal route — to ensure that increased sanctioning power does not come at the expense of due process.

4.3. Mandate universal, time-bound breach notification

The breach-notification duty introduced for the financial sector in 2025 should be extended, through amendment of the Law "On Personal Data," to all operators of digital platforms that process personal data at scale, with a defined notification window (for example, seventy-two hours, mirroring the GDPR standard) both to the supervisory authority and, where risk to individuals is significant, to the affected data subjects themselves. This would have provided a clearer public-accountability mechanism during the 2026 incidents, where confirmation and clarification of the facts took weeks.

4.4. Build risk-based, proactive supervision of digital platforms

Rather than relying primarily on complaint-driven investigation, the future consolidated authority should adopt a risk-based inspection plan, prioritizing platforms that process high volumes of sensitive data — banking and payment applications, ride-hailing and delivery services, healthcare portals, and e-government systems — following the PIPC's practice of publishing annual, sector-targeted enforcement priorities. This would allow limited regulatory resources to be directed where the potential harm from a breach is greatest.

4.5. Calibrate localization rules to risk, not blanket geography

The 2026 reform that replaced blanket data-localization with a tiered approach — permitting foreign storage subject to adequacy findings, standard contractual clauses, or recognized international standards, while keeping biometric and telecom data domestic — represents a legally sound direction and should be extended methodically to other sectors, accompanied by published, transparent criteria for what constitutes an "adequate" foreign

[13]Chambers and Partners, ibid. — on the PIPC's first adequacy decision for the EU, announced September 2025.

jurisdiction, to avoid case-by-case discretion that could undermine legal certainty for platform operators.

4.6. Strengthen inter-agency coordination protocols

Finally, a binding coordination protocol between the future data-protection authority, the Cybersecurity Center, sectoral regulators (in banking, telecommunications, and healthcare), and law-enforcement bodies should define, in advance, who leads an investigation, within what timeframe, and how findings are communicated to the public — reducing the risk of the kind of conflicting or delayed public statements observed during the 2026 breach allegations.

5. CONCLUSION

The comparative analysis conducted in this article shows that the effectiveness of personal-data protection on digital platforms depends less on the mere existence of a data-protection law — Uzbekistan has had one since 2019 — than on the institutional architecture that enforces it. The European Union's independent, fine-empowered Data Protection Authorities and the Republic of Korea's evolution of the PIPC from an advisory panel into a fully independent enforcement agency both demonstrate that institutional independence, proportionate sanctioning power, and proactive, risk-based supervision are what convert a data-protection statute from a declarative document into an operative safeguard.

Uzbekistan's 2025–2026 reforms — breach-notification duties in the financial sector and a more flexible, risk-tiered approach to data localization — indicate that the legislator is moving in this direction, but the events of early 2026, including the alleged large-scale leak of citizens' data and the separate incident implicating the Cybersecurity Center's own personnel data, suggest that institutional consolidation, clearer sanctioning authority, and universal breach-notification rules remain unfinished tasks. Addressing them would bring Uzbekistan's regulatory framework closer to the international standards it seeks to align with, while directly serving the constitutional guarantee of privacy that underlies the entire field.

REFERENCES

1. Constitution of the Republic of Uzbekistan (new edition), effective 1 May 2023. https://lex.uz/uz/docs/-6445145
2. Law of the Republic of Uzbekistan "On Personal Data" No. ZRU-547, 2 July 2019. https://lex.uz/docs/-4396419
3. Law of the Republic of Uzbekistan "On Electronic Commerce" No. ZRU-792, 29 September 2022. https://lex.uz/docs/-6213382
4. Law of the Republic of Uzbekistan "On Telecommunications" No. ZRU-1015, 28 December 2024.https://www.lex.uz/uz/docs/-7283071
5. Presidential Decree of the Republic of Uzbekistan No. PQ-153, 30 April 2025 https://lex.uz/uz/docs/-7511145
6. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 71, 8 February 2020, "On Approval of the Regulation on the State Register of Personal Data Bases." https://lex.uz/ru/docs/-4729730
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
8. Personal Information Protection Act of the Republic of Korea (as amended 2020, 2023, 2025).https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG
9. DLA Piper, Data Protection Laws of the World Handbook, Uzbekistan chapter, 2025 edition.https://www.dlapiperdataprotection.com/index.html?t=law&c=UZ

10. Legal500, “Personal Data Compliance in Uzbekistan,” 2025. https://www.legal500.com/developments/thought-leadership/personal-data-compliance-in-uzbekistan/
11. The Times of Central Asia, “Uzbekistan Eases Data Localization Rules to Support Global Payment Platforms,” February 2026. https://timesca.com/uzbekistan-eases-data-localization-rules-to-support-global-payment-platforms/
12. Kiberxavfsizlik markazi (Cybersecurity Center of the Republic of Uzbekistan), official website. https://csec.uz/uz/
13. GDPR-EU.org, “Who Is Responsible for Enforcing the GDPR?” https://www.gdpreu.org/who-is-responsible-for-enforcing-the-gdpr/
14. Chambers and Partners, “Data Protection & Privacy 2026 — South Korea,” Global Practice Guides.https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2026/south-korea/trends-and-developments