4 INTERNATIONAL AND COMPARATIVE LAW
ХАЛЫҚАРАЛЫҚ ЖӘНЕ САЛЫСТЫРМАЛЫ ҚҰҚЫҚ
МЕЖДУНАРОДНОЕ И СРАВНИТЕЛЬНОЕ ПРАВО

UDC 342.72/.73
IRSTI 10.19.61
JEL K14

https://doi.org/10.46914/2959-4197-2025-1-2-7-53-62

DYUSSEBAYEV Z.S.,*[1]
PhD student.
*e-mail: z.dyussebayev@turan-edu.kz
ORCID ID: 0009-0009-5137-9835
ALAYEVA G.T.,[1]
c.l.s., professor.
e-mail: g.alayeva@turan-edu.kz
ORCID ID: 0000-0003-1672-2238
DZHUMABAYEVA K.A.,[1]
PhD, associate professor.
e-mail: k.jumabaeva@turan-edu.kz
ORCID ID: 0000-0002-5483-3783
STVOL M.,[2]
PhD, professor.
e-mail: gulasmz@gmail.com
ORCID ID: 0000-0002-6624-4505
[1]Turan University,
Almaty, Kazakhstan
[2]Gdansk University,
Gdansk, Poland

PERSONAL DATA AND DIGITAL SECURITY: PRACTICAL APPROACHES TO REFORMING KAZAKHSTAN'S LEGISLATION IN LIGHT OF THE GDPR

Abstract

This article examines the current state and development prospects of Kazakhstan's personal data protection system through a comprehensive comparative legal analysis with the European Union's General Data Protection Regulation (GDPR). The study identifies key deficiencies in Kazakhstan's legal and institutional framework, particularly the limited scope of enforcement mechanisms and the inadequacy of administrative penalties in deterring violations. Emphasis is placed on the extraterritorial reach, strict compliance requirements, and high sanctions under the GDPR, which collectively contribute to its global influence. Drawing from case studies, expert policy reports, and regulatory practices, the article underscores the importance of strengthening legal accountability, enhancing state oversight functions, and establishing proactive enforcement capabilities. Special attention is given to the role of digital sovereignty and the integration of internationally recognized standards into Kazakhstan's legislative environment. The analysis also highlights domestic corporate practices that are beginning to align with GDPR principles, using Air Astana as a pioneering example. The article concludes by offering concrete policy recommendations, including the

introduction of mandatory breach notification procedures and legislative reform to empower supervisory authorities. These measures are essential for creating a more transparent, secure, and rights-based approach to personal data governance in Kazakhstan.

Keywords: personal data protection, digital security, data breaches, legal accountability, state oversight, administrative fines, comparative law.

Introduction

The question of cybersecurity for citizens has emerged as one of the most pressing concerns on the global agenda, particularly in the context of the accelerating pace of digitalization. As digital technologies continue to evolve and permeate nearly every aspect of public and private life – from finance and healthcare to education, public administration, and interpersonal communication – their benefits are paralleled by significant risks. These include, most notably, the unauthorized access, misuse, or loss of sensitive data, which may result in severe infringements on individual rights and freedoms. Consequently, the development of reliable mechanisms to ensure cybersecurity is no longer a matter of technical infrastructure alone but has become a critical legal and policy issue for national governments and international institutions alike.

Cybersecurity is a multifaceted and interdisciplinary field that encompasses a wide range of technical, legal, social, and ethical dimensions. Given the complexity of the topic, it is not feasible to explore all aspects within the scope of a single study. Therefore, this paper concentrates on one of the most essential components of cybersecurity – the protection of personal data. This dimension is especially relevant in an era when data has become a new form of capital, and where its collection, processing, and exchange play a pivotal role in both commercial strategies and public governance.

The omnipresence of automated data processing in digital communication implies that vast quantities of personal information are constantly being generated, transmitted, and stored. These processes inherently involve legal and ethical questions, particularly regarding who controls the data, how it is used, and what safeguards are in place to prevent abuse. As information and communication technologies (ICTs) have become more sophisticated, the transmission of personal data has transcended national borders, raising complex issues of jurisdiction, legal accountability, and regulatory coordination. This transnational nature of data flows further underscores the need for harmonized legal approaches and the adaptation of international standards into national legislative frameworks.

In this context, personal data protection must be viewed not only as a matter of information security but as a fundamental human rights issue rooted in the right to privacy and the integrity of individual identity. The legal understanding of privacy has long preceded the formal codification of personal data protection laws. However, the exponential growth in the volume and sensitivity of data collected – often without the knowledge or informed consent of the data subject – has compelled lawmakers around the world to develop new legal instruments and regulatory bodies to oversee and enforce data protection regimes.

In Kazakhstan, the definition of personal data is codified in Article 1(2) of Law No. 94–V "On Personal Data and Their Protection," enacted on May 21, 2013. According to the law, personal data refers to information relating to an identified or identifiable individual, recorded in electronic, paper–based, or other material formats [1]. This aligns conceptually with the definition set forth in the General Data Protection Regulation (GDPR) of the European Union, which describes personal data as any information relating to an identified or identifiable natural person – one who can be identified, directly or indirectly, through identifiers such as names, identification numbers, location data, online identifiers, or characteristics specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity [2].

Drawing comparisons between Kazakhstan's national legal framework and European regulations is not only methodologically relevant but practically important. It allows for a comprehensive assessment of how personal data is protected under differing legal systems and provides a benchmark for evaluating Kazakhstan's alignment with international best practices. Moreover, such comparative analysis can reveal gaps in the current regulatory environment and offer insights into how selected

elements of the GDPR might be integrated into Kazakhstan's legal system to enhance personal data protection.

In addition to legislative analysis, attention must also be paid to the institutional and procedural aspects of data protection. This includes understanding how laws are implemented in practice, the mandates and effectiveness of regulatory bodies, and the level of accountability among stakeholders involved in handling personal data. Recent developments in Kazakhstan suggest that improving accountability, especially among data controllers and processors, is vital to strengthening the country's data protection regime and ensuring public trust in digital governance.

Materials and methods

This study, entitled "Ensuring the Protection of Personal Data and the Need to Increase the Responsibility of Specific Stakeholders," employs a comprehensive methodological framework combining legal, empirical, and comparative research techniques. The aim is to evaluate the current state of personal data protection in Kazakhstan and identify pathways for regulatory improvement through the adoption of international best practices.

The method of legal analysis and synthesis forms the foundation of this research. This approach entails a detailed examination of Kazakhstan's key legislative act in the area of data protection – the Law No. 94–V "On Personal Data and Their Protection" – as well as the European Union's General Data Protection Regulation (GDPR). A systematic review of legal texts, secondary literature, and scholarly commentaries was conducted to identify core principles, definitions, and regulatory mechanisms. Analysis was used to deconstruct legal norms and examine their scope, content, and application. Synthesis, in turn, enabled the consolidation of findings into coherent arguments regarding the strengths and deficiencies of Kazakhstan's legal regime, as well as the practical steps necessary for its improvement.

The comparative legal method was applied to juxtapose Kazakhstan's legal provisions against those enshrined in the GDPR, one of the world's most advanced and influential data protection instruments. This method allows for a nuanced understanding of where Kazakhstan's legal framework aligns with or diverges from international standards. It also provides insights into which elements of the GDPR might be realistically adapted within the Kazakh context, taking into account local legal culture, institutional capacity, and socio–political considerations.

The systemic approach was utilized to conceptualize the personal data protection ecosystem as an integrated network of interdependent elements. These include individual data subjects, data controllers and processors, database owners, regulatory bodies, state monitoring institutions, legal liability mechanisms, and channels of redress. By treating these elements as a unified system, the method facilitates the identification of weaknesses or failures at specific nodes, thereby enabling targeted recommendations for improving data security and institutional accountability.

The empirical method, which includes the analysis of statistical data and enforcement practices, was employed to provide a quantitative basis for the research findings. Data on incidents of data breaches, administrative and criminal proceedings, and sanctions imposed for violations of data protection laws in Kazakhstan were collected and analyzed. Moreover, a selection of court rulings was examined to assess how legal norms are interpreted and enforced in practice. This component of the study serves to illustrate the real–world implications of legal frameworks and the extent to which they are capable of deterring misconduct and ensuring justice for affected individuals.

Taken together, these methodological tools ensure a holistic and multi–perspective analysis of the legal, institutional, and societal aspects of personal data protection in Kazakhstan. They also support the formulation of evidence–based policy recommendations aimed at improving the national regulatory framework and strengthening its compliance with international standards. Ultimately, the combination of normative and empirical research approaches enhances the study's relevance and applicability in both academic and policymaking contexts.

Results and discussion

The core objective of the Law of the Republic of Kazakhstan "On Personal Data and Their Protection" – and the legal system constructed upon it – is to safeguard the fundamental rights and freedoms of individuals in the course of the collection and processing of their personal information [1]. This protection is intended to be achieved through a combination of legal, organizational, and technical measures, the effectiveness of which is guaranteed by the state itself. The Law outlines the responsibilities and obligations of various actors involved in personal data processes – including collection, accumulation, processing, storage, dissemination, cross–border transfer, usage, and destruction – ensuring that each stage is carried out in full compliance with national legal standards.

Among its key provisions, the Law establishes the rights and duties of personal data subjects, owners of databases, and data operators. However, the mere presence of legal norms is insufficient – their effective enforcement and rigorous oversight are vital. To this end, the Law delegates a range of competencies to an authorized public body, which is tasked with exercising state control over compliance with personal data legislation in Kazakhstan.

According to Order No. 169/NK issued on July 22, 2019, by the Acting Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan, the Committee for Information Security – a subordinate body of the Ministry – is entrusted with regulatory, implementation, and supervisory functions related to information security in the field of digitalization, including the protection of personal data [3]. Within this institutional structure, the Department for Personal Data Protection (hereinafter – the Department of the Committee for Information Security under the Ministry of Digital Development, Innovation and Aerospace Industry, or "PDP Department of CIS MDDIAI RK") is directly responsible for the implementation of relevant state functions, including monitoring and control over compliance with the Law.

In this context, state control refers to the activities of supervisory bodies aimed at verifying and overseeing the compliance of data controllers and other subjects with the legal requirements established by Kazakhstan's legislation [4]. Such control measures may be executed through both scheduled and unscheduled inspections. Scheduled audits are conducted based on an annually approved plan, while unscheduled inspections are initiated only upon receiving complaints from individuals or legal entities alleging violations of their rights, or upon instructions from law enforcement authorities [5].

In the event that legal violations are uncovered during these inspections, responsible entities may face administrative or criminal liability, depending on the gravity of the offense. Under Article 79 of the Code of Administrative Offenses (CAO RK), individuals or organizations that breach the provisions of the Law may be subject to administrative fines of up to 1,000 monthly calculation indices (MCI), amounting to approximately 3,692,000 tenge [6]. This constitutes the maximum non–criminal penalty applicable for data protection violations. For offenses of a more serious nature, criminal liability is established under Article 147 of the Criminal Code of the Republic of Kazakhstan (CC RK), which prescribes sanctions ranging from fines of up to 5,000 MCI (18,460,000 tenge) to corrective or community service, and even imprisonment of up to seven years [7].

However, the vast majority of data protection violations in Kazakhstan are classified as administrative rather than criminal offenses. As a result, most entities that fail to comply with the Law are penalized only through administrative fines, which, for large–scale commercial enterprises, may represent a negligible financial burden. The punitive effect of such sanctions is thus significantly diminished, particularly when weighed against the potential damage and financial harm caused to citizens through unauthorized data leaks or unlawful processing.

A recent example illustrates this disproportionality: in March 2024, the personal data of over two million Kazakh citizens – clients of the microfinance organization zaimer.kz (LLP "MFO Robocash.kz") – was leaked. Although the incident affected a substantial portion of the population, the company was subjected only to the maximum administrative fine available under the CAO – 1,000 MCI (3,692,000 tenge), a figure unlikely to serve as a serious deterrent.

In contrast, the European Union's GDPR regime establishes significantly more stringent standards for data protection and accountability. Article 83 of the GDPR sets out the framework for administrative fines. Under Article 83(4), for non–severe breaches related to the obligations of controllers and processors, fines may reach up to €10 million or 2% of the total worldwide annual turnover, whichever

is higher. In more serious cases – such as violations of data subject rights, fundamental data processing principles, or conditions for cross–border data transfers – fines can climb to €20 million or 4% of global annual revenue, again depending on which figure is greater [2].

This structure ensures that no upper ceiling exists for GDPR fines, thereby compelling organizations – especially multinational corporations – to invest in robust data protection mechanisms. In 2023, the tech giant Meta (formerly Facebook) received a record–breaking €1.2 billion fine for multiple GDPR violations committed between 2020 and 2023 [8]. Such precedents exemplify the EU's zero–tolerance approach to non–compliance and demonstrate how heavy sanctions can effectively influence corporate behavior.

By comparison, the difference in potential financial penalties between the EU and Kazakhstan – €20 million or 4% of annual global turnover versus a maximum of approximately €7,500 (equivalent to 3.7 million tenge) – renders any direct comparison futile. The rigorous enforcement and severe penalty structure embedded in the GDPR have contributed not only to its domestic effectiveness but also to its global influence. The GDPR is widely recognized as one of the most advanced and impactful legal instruments for personal data protection worldwide.

Comparative analysis of global data protection frameworks confirms the relative stringency of the GDPR, particularly in areas of consent, extraterritoriality, and enforcement. As noted by Olamide and James, the GDPR's clarity on data subject rights and its comprehensive penalty structure distinguish it from laws like the CCPA and China's PIPL [9].

Recognizing the shortcomings of Kazakhstan's current system, domestic experts have also called for legal reform. In October 2022, a policy study was conducted under the project "Institution for the Development of Personal Data Protection," led by Ruslan Daiyrbekov and Yelzhan Kabyshev and supported by the Eurasia Foundation through the "Social Innovation in Central Asia" program funded by USAID. Using comparative legal analysis, the study examined the procedural response mechanisms to data breaches in both Kazakhstan and foreign jurisdictions, focusing in particular on alignment with GDPR principles.

As a result of the study, the experts proposed a number of recommendations aimed at improving Kazakhstan's data protection system. One critical issue identified was the lack of legal authority for the authorized body (PDP Department of CIS MDDIAI RK) to initiate inspections independently. The current framework only allows for reactive, not proactive, oversight – a gap that undermines the overall effectiveness of enforcement.

Among the proposed legislative reforms was the introduction of a legal definition for the term "data breach" to enable the enforcement of data subject rights and facilitate the prosecution of violators. Furthermore, the experts advocated for the mandatory notification of all data breaches to both supervisory authorities and affected individuals, as well as the implementation of legal responsibility for failure to report such breaches [10]. These reforms are essential for establishing an accountable and transparent system of data protection and for fostering public trust in Kazakhstan's digital governance infrastructure.

In his article "Digital Sovereignty as a Fundamental Component of Contemporary Cybersecurity," A.M. Saitbekov provides a detailed examination of the role of state control within the digital sphere. The author argues that there is a critical need for the development of normative regulations that define the procedures and mechanisms of governmental oversight in cyberspace. According to Saitbekov, such regulatory efforts must primarily aim to protect individuals from unlawful interference and digital threats [11]. We fully endorse the author's position regarding the necessity of establishing a clearly structured framework for state oversight. The protection of personal data is inseparably linked to broader issues of digital security, and thus the incorporation of Saitbekov's research into the present analysis is both appropriate and justified.

This position aligns with broader academic discussions on digital sovereignty, where scholars argue that national regulatory systems must be recognized and integrated into the fabric of global digital governance. Singh contends that building a fair and effective digital architecture at the global level requires institutional mechanisms for mutual recognition of sovereign regulatory frameworks [12].

The global impact of the General Data Protection Regulation (GDPR) stems not merely from its content but from the scale and scope of its extraterritorial application. Although the GDPR formally applies only to the residents and citizens of the European Union, its influence inevitably extends

beyond EU borders. Any organization – regardless of geographic location – that seeks to offer services to EU citizens or process their personal data must comply with GDPR provisions [13]. This dynamic reflects a natural evolution of market behavior under conditions of global competition. In today's environment, compliance with robust data protection laws such as the GDPR is a prerequisite for accessing and maintaining a presence in the European market.

Multinational corporations including Google, Facebook (Meta), Amazon, Apple, and Microsoft have incorporated GDPR standards into their internal policies and privacy frameworks. For example, Apple's Privacy Policy explicitly regulates the cross–border transfer of personal data among its affiliated entities across different jurisdictions. Users are required to consent to the processing of their data by Apple entities located in other countries. However, for data originating from the EU, Apple enforces special contractual clauses developed in accordance with GDPR standards. These clauses govern data transfers and guarantee compliance with EU–level legal protections [14].

Organizations that adhere to GDPR requirements enjoy a distinct competitive advantage over those that fail to meet these legal standards. Not only does compliance reduce the risk of reputational damage and financial penalties, but it also signals corporate responsibility, transparency, and a commitment to user rights. Consequently, GDPR–aligned data protection practices have become a market differentiator and a hallmark of trustworthy governance.

In light of the significance and reach of the GDPR, its gradual adoption by Kazakhstani enterprises – particularly those engaged in international business – appears both expected and strategically sound. A notable example is the national airline Air Astana, which was among the first Kazakhstani companies to integrate GDPR norms into its corporate data governance documentation following the regulation's enforcement. The company's updated Privacy Policy now reflects the core principles of both the national Law of the Republic of Kazakhstan and the GDPR. For instance, the policy defines Air Astana JSC as the data controller for any personal information processed by the company. In cases where flight reservations include segments operated by partner airlines, those airlines are also designated as independent data controllers. The same designation applies to third–party service providers such as hotels, car rental agencies, or ticketing platforms like Ticketon [15].

These legal designations – distinguishing among multiple independent controllers – demonstrate a clear alignment with GDPR logic, where responsibilities are clearly apportioned, and legal accountability is structured. Air Astana's compliance model illustrates how the principles of the GDPR can be effectively adapted within Kazakhstan's legal and corporate contexts.

As noted by Edwards and Veale, the GDPR stands out for its structured, transparent approach to regulating data subject rights and its potential for global normative influence due to the universality of its principles [16].

Following Air Astana's lead, many other Kazakhstani companies – particularly those with operational or ownership ties to the EU – have also begun to implement GDPR–aligned standards within their own data processing frameworks. As Coche, Kolk, and Ocelík (2024) emphasize, understanding the legal diversity in national data governance regimes is crucial for effective digitalization and cross-border business operations [17]. Whether due to direct market engagement with the EU, affiliation with European partners, or the involvement of EU citizens in corporate structures, these companies have recognized the necessity of GDPR compliance. As a result, the European legal model of personal data protection is progressively becoming a benchmark for responsible business conduct in Kazakhstan.

Conclusion

In conclusion, the critical importance of further developing the domain of personal data protection cannot be overstated. At the heart of an effective data protection system lies a legislative foundation that is aligned with global standards, coupled with the proper implementation of legal norms and a heightened sense of accountability among all actors involved in data processing. Without these three pillars – legal adequacy, practical enforcement, and personal responsibility – data protection systems risk becoming nominal rather than functional.

In this regard, the personal data protection framework in Kazakhstan requires ongoing in–depth analysis, legal modernization, and structured engagement with international best practices. Comparative analysis with the European Union's advanced data protection regime – founded on the General Data

Protection Regulation (GDPR) – reveals a significant gap between Kazakhstan's current model and globally recognized standards. The EU's experience provides a practical and replicable model that can inform and guide meaningful reforms in Kazakhstan's legal and institutional architecture.

Based on the comparative legal study of the legislation of the Republic of Kazakhstan and the European Union in the field of personal data protection, this research has identified a key vector for national reform: enhancing the level of responsibility among stakeholders involved in the collection, processing, storage, use, and transfer of personal data. Strengthening accountability is not merely a legal imperative, but a strategic priority that underpins data security, public trust, and digital sovereignty.

One of the most effective mechanisms for increasing accountability is the tightening of sanctions for violations of data protection laws. As demonstrated throughout this study, the current maximum administrative fine in Kazakhstan – set at approximately 3.7 million tenge – is largely symbolic and fails to reflect the scale of potential harm that can arise from unlawful data breaches or unauthorized processing of citizens' personal information. In contrast, the GDPR has introduced a robust penalty regime that incentivizes compliance through the threat of proportionate and dissuasive financial penalties.

Substantial fines have proven to be a powerful driver of change, compelling organizations to implement comprehensive technological and organizational safeguards. This approach has been notably successful within the European context, and in many ways has exceeded expectations, as the influence of the GDPR now extends well beyond EU borders. Its principles have shaped corporate policies worldwide, thereby setting a de facto global standard for personal data protection.

As Kazakhstan continues to integrate into the global digital economy, aligning its national data protection framework with international norms – particularly those enshrined in the GDPR – represents not only a legal modernization effort but a fundamental step toward ensuring the rights of its citizens in the digital age.

REFERENCES

1 Закон Республики Казахстан от 21 мая 2013 г. № 94-V «О персональных данных и их защите». URL: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 01.04.2025)

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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. No. 119. P. 1–88.

3 Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 22 июля 2021 г. № 169/НҚ «Об утверждении Положения о республиканском государственном учреждении «Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан». URL: https://online.zakon.kz/Document/?doc_id=33938407 (дата обращения: 01.04.2025)

4 Кодекс Республики Казахстан от 29 октября 2015 года № 375-V «Предпринимательский кодекс Республики Казахстан». URL: https://online.zakon.kz/Document/?doc_id=38259854 (дата обращения: 01.04.2025)

5 Дайырбеков Р., Кабышев Е. Сравнительно-правовой анализ национального и зарубежного законодательства по оперативному реагированию при утечке персональных данных. – Астана: Институт развития защиты персональных данных, Фонд Евразия, 2023. – 42 с.

6 Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 г. № 235-V. URL: https://adilet.zan.kz/rus/docs/K1400000235 (дата обращения: 01.04.2025)

7 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V. URL: https://online.zakon.kz/Document/?doc_id=31575252&pos=2351;-38#pos=2351;-38 (дата обращения: 01.04.2025)

8 Кабышев Е. Утечки персональных данных: мировой и казахстанский аспекты // Ландшафт цифровых прав и свобод. URL: https://drfl.kz/ru/utechki-personalnykh-dannykh/ (дата обращения: 01.04.2025)

9 Olamide B., James A. Comparative Analysis of CCPA, GDPR, and Other Data Protection Regulations. 2023. URL: https://www.researchgate.net/publication/389883174 (accessed: 01.04.2025)

10 META оштрафована за нарушение норм GDPR на рекордные 1,2 млрд евро: почему это произошло и чего ждать контролерам? – 2023. URL: https://revera.legal/en/info-centr/news-and-analytical-materials/1333-meta-oshtrafovana-za-narushenie-norm-gdpr-pochemu-eto-proizoshlo-i-chego-zhdat-kontroleram/ (дата обращения: 01.04.2025)

11 Apple. Privacy Policy dated September 18, 2024. URL: https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-ru.pdf (accessed: 01.04.2025)

12 Политика конфиденциальности АО «Эйр Астана». URL: https://airastana.com/kaz/ru-ru/Informatsiia/Pravila-i-usloviia/Politika-konfidentsialnosti (дата обращения 01.04.2025)

13 Edwards L., Veale M. Navigating Privacy: A Global Comparative Analysis of the GDPR and Other Major Privacy Laws // Computer Law & Security Review. 2023. Vol. 50. DOI: 10.1016/j.clsr.2023.105832.

14 Coche E., Kolk A., Ocelík V. Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business // Journal of International Business Policy. 2024. Vol. 7. P. 112–127. DOI: 10.1057/s42214-023-00172-1.

REFERENCES

1 Zakon Respubliki Kazahstan ot 21 maja 2013 g. № 94-V «O personal'nyh dannyh i ih zashhite». URL: https://adilet.zan.kz/rus/docs/Z1300000094 (data obrashhenija: 01.04.2025). (In Russian).

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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. No.119. P. 1–88. (In English)

3 Prikaz i.o. Ministra cifrovogo razvitija, innovacij i ajerokosmicheskoj promyshlennosti Respubliki Kazahstan ot 22 ijulja 2021 g. No. 169/NQ «Ob utverzhdenii Polozhenija o respublikanskom gosudarstvennom uchrezhdenii «Komitet po informacionnoj bezopasnosti Ministerstva cifrovogo razvitija, innovacij i ajerokosmicheskoj promyshlennosti Respubliki Kazahstan». URL: https://online.zakon.kz/Document/?doc_id=33938407 (data obrashhenija: 01.04.2025). (In Russian).

4 Kodeks Respubliki Kazahstan ot 29 oktjabrja 2015 goda No. 375-V «Predprinimatel'skij kodeks Respubliki Kazahstan». URL: https://online.zakon.kz/Document/?doc_id=38259854 (data obrashhenija: 01.04.2025). (In Russian).

5 Dajyrbekov R., Kabyshev E. (2023) Sravnitel'no-pravovoj analiz nacional'nogo i zarubezhnogo zakonodatel'stva po operativnomu reagirovaniju pri utechke personal'nyh dannyh. Astana: Institut razvitija zashhity personal'nyh dannyh, Fond Evrazija. 42 p. (In Russian).

6 Kodeks Respubliki Kazahstan ob administrativnyh pravonarushenijah ot 5 ijulja 2014 g. No. 235-V. URL: https://adilet.zan.kz/rus/docs/K1400000235 (data obrashhenija: 01.04.2025). (In Russian).

7 Ugolovnyj kodeks Respubliki Kazahstan ot 3 ijulja 2014 goda No. 226-V. URL: https://online.zakon.kz/Document/?doc_id=31575252&pos=2351;-38#pos=2351;-38 (data obrashhenija: 01.04.2025). (In Russian).

8 Kabyshev E. (2023) Utechki personal'nyh dannyh: mirovoj i kazahstanskij aspekty // Landshaft cifrovyh prav i svobod. URL: https://drfl.kz/ru/utechki-personalnykh-dannykh/ (data obrashhenija: 01.04.2025)

9 Olamide B., James A. (2023) Comparative Analysis of CCPA, GDPR, and Other Data Protection Regulations. URL: https://www.researchgate.net/publication/389883174 (accessed: 01.04.2025). (In English).

10 META oshtrafovana za narushenie norm GDPR na rekordnye 1,2 mlrd evro: pochemu jeto proizoshlo i chego zhdat' kontroleram? 2023. URL: https://revera.legal/en/info-centr/news-and-analytical-materials/1333-meta-oshtrafovana-za-narushenie-norm-gdpr-pochemu-eto-proizoshlo-i-chego-zhdat-kontroleram/ (data obrashhenija: 01.04.2025). (In Russian).

11 Apple. Privacy Policy dated September 18, 2024. URL: https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-ru.pdf (access date: 01.04.2025). (In English).

12 Politika konfidencial'nosti AO «Jejr Astana». URL: https://airastana.com/kaz/ru-ru/Informatsiia/Pravila-i-usloviia/Politika-konfidentsialnosti (data obrashhenija 01.04.2025). (In Russian).

13 Edwards L., Veale M. (2023) Navigating Privacy: A Global Comparative Analysis of the GDPR and Other Major Privacy Laws // Computer Law & Security Review. Vol. 50. DOI: 10.1016/j.clsr.2023.105832. (In English).

14 Coche E., Kolk A., Ocelík V. (2024.) Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business // Journal of International Business Policy. Vol. 7. P. 112–127. DOI: 10.1057/s42214-023-00172-1. (In English).

ДЮСЕБАЕВ Ж.С.,*[1]
докторант.
*e-mail: z.dyussebayev@turan-edu.kz
ORCID ID: 0009-0009-5137-9835
АЛАЕВА Г.Т.,[1]
з.ғ.к., профессор.
e-mail: alaevagulnaz@mail.ru
ORCID ID: 0000-0003-1672-2238
ДЖУМАБАЕВА К.А.,[1]
PhD, қауымдастырылған профессор.
e-mail: k.jumabaeva@turan-edu.kz
ORCID ID: 0000-0002-5483-3783
СТВОЛ М.,[2]
PhD, профессор.
e-mail: gulasmz@gmail.com
ORCID ID: 0000-0002-6624-4505
[1]«Тұран» университеті,
Алматы қ., Қазақстан
[2]Гданьск университеті,
Гданьск қ., Польша

ДЕРБЕС ДЕРЕКТЕР МЕН ЦИФРЛЫҚ ҚАУІПСІЗДІК: ҚАЗАҚСТАН ЗАҢНАМАСЫН GDPR АЯСЫНДА РЕФОРМАЛАУДЫҢ ПРАКТИКАЛЫҚ ТӘСІЛДЕРІ

Аңдатпа

Бұл мақалада Қазақстан Республикасындағы дербес деректерді қорғау жүйесінің қазіргі жағдайы мен даму перспективалары Еуропалық Одақтың Жалпы деректерді қорғау регламентімен (GDPR) салыстырмалы құқықтық талдау арқылы зерттеледі. Зерттеу нәтижесінде Қазақстанның құқықтық және институционалдық жүйесінде бірқатар кемшіліктер анықталды, атап айтқанда, мәжбүрлеу тетіктерінің шектеулігі мен құқықбұзушылықтардың алдын алуда әкімшілік айыппұлдардың жеткіліксіздігі. GDPR-дің экстерриториялық әсері, қатаң талаптары және жоғары санкциялары оның жаһандық ықпалын арттырады. Кейстік зерттеулер, сараптамалық есептер мен тәжірибелер негізінде құқықтық жауапкершілікті күшейту, мемлекеттің қадағалау функцияларын жетілдіру және тиімді мәжбүрлеу механизмдерін құру қажеттілігі атап өтіледі. Мақалада цифрлық егемендіктің маңызы мен халықаралық стандарттарды Қазақстан заңнамасына интеграциялау мәселесіне ерекше назар аударылады. Сонымен қатар, GDPR қағидаттарына жақындап келе жатқан отандық корпоративтік тәжірибелер, мысалы, Air Astana компаниясының тәжірибесі талданады. Мақала міндетті түрде деректердің бұзылуы туралы хабарлау рәсімдерін енгізу және бақылаушы органдардың өкілеттіктерін кеңейтуге бағытталған заңнамалық реформалар сияқты нақты саясаттық ұсыныстармен қорытындыланады. Бұл шаралар Қазақстанда дербес деректерді басқарудың ашық, қауіпсіз және құқыққа негізделген тәсілін қалыптастыру үшін маңызды.

Тірек сөздер: дербес деректерді қорғау, цифрлық қауіпсіздік, деректердің таралуы, құқықтық жауапкершілік, мемлекеттік бақылау, әкімшілік айыппұлдар, салыстырмалы құқық.

ДЮСЕБАЕВ Ж.С.,*[1]
докторант.
*e-mail: z.dyussebayev@turan-edu.kz
ORCID ID: 0009-0009-5137-9835
АЛАЕВА Г.Т.,[1]
к.ю.н., профессор.
e-mail: alaevagulnaz@mail.ru
ORCID ID: 0000-0003-1672-2238
ДЖУМАБАЕВА К.А.,[1]
PhD, ассоциированный профессор.
e-mail: k.jumabaeva@turan-edu.kz
ORCID ID: 0000-0002-5483-3783
СТВОЛ М.,[2]
PhD, профессор.
e-mail: gulasmz@gmail.com
ORCID ID: 0000-0002-6624-4505
[1]Университет «Туран»,
г. Алматы, Казахстан
[2]Гданьский университет,
г. Гданьск, Польша

ПЕРСОНАЛЬНЫЕ ДАННЫЕ И ЦИФРОВАЯ БЕЗОПАСНОСТЬ: ПРАКТИЧЕСКИЕ ПОДХОДЫ К РЕФОРМЕ ЗАКОНОДАТЕЛЬСТВА КАЗАХСТАНА С УЧЕТОМ GDPR

Аннотация

В статье рассматривается текущее состояние и перспективы развития системы защиты персональных данных в Республике Казахстан на основе комплексного сравнительно-правового анализа с Общим регламентом по защите данных Европейского союза (GDPR). В ходе исследования выявлены ключевые недостатки в правовой и институциональной системе Казахстана, особенно в части ограниченных механизмов принуждения и недостаточной эффективности административных санкций в предотвращении нарушений. Особое внимание уделено экстерриториальному действию, строгим требованиям соблюдения и высоким штрафам, предусмотренным GDPR, что усиливает его глобальное влияние. На основе кейс-исследований, экспертных докладов и анализа регуляторной практики подчеркивается необходимость усиления юридической ответственности, расширения надзорных функций государства и создания действенных механизмов принудительного исполнения. Особый акцент сделан на значении цифрового суверенитета и интеграции международно признанных стандартов в законодательную среду Казахстана. Также анализируются отдельные примеры отечественной корпоративной практики, приближающейся к принципам GDPR, в частности деятельность компании «Air Astana». В завершение статьи даны конкретные рекомендации по государственной политике, включая введение обязательного уведомления о нарушении безопасности персональных данных и проведение законодательной реформы с целью расширения полномочий надзорных органов. Эти меры необходимы для формирования более прозрачного, безопасного и ориентированного на права человека подхода к управлению персональными данными в Казахстане.

Ключевые слова: защита персональных данных, цифровая безопасность, утечка данных, правовая ответственность, государственный контроль, административные штрафы, сравнительное право.

Article submission date: 29.05.2025