UDC 342.7
Doi: 10.32518/sals4.2024.90

Соціально-правові студії. 2024. Т. 7, № 4
Social & Legal Studios. 2024. Vol. 7, No. 4

Protection of information about employee's personal data in the Republic of Kazakhstan

Fatima Syrlybayeva*
Postgraduate Student
L.N. Gumilyov Eurasian National University
010008, 2 Satpayev Str., Astana, Republic of Kazakhstan
https://orcid.org/0009-0009-2349-0894

Xeniya Kassymova
Postgraduate Student
L.N. Gumilyov Eurasian National University
010008, 2 Satpayev Str., Astana, Republic of Kazakhstan
https://orcid.org/0000-0001-7759-209X

Elmira Omarova
PhD, Associate Professor
L.N. Gumilyov Eurasian National University
010008, 2 Satpayev Str., Astana, Republic of Kazakhstan
https://orcid.org/0000-0002-2927-7164

Bakyt Zhussipova
PhD, Associate Professor
L.N. Gumilyov Eurasian National University
010008, 2 Satpayev Str., Astana, Republic of Kazakhstan
https://orcid.org/0000-0002-2710-2950

Enlik Nurgalieva
Full Doctor, Professor
L.N. Gumilyov Eurasian National University
010008, 2 Satpayev Str., Astana, Republic of Kazakhstan
https://orcid.org/0009-0002-0568-0765

Abstract. The relevance of this study is conditioned by an increase in the number of cases of leakage of personal data of citizens, which indicates a low level of protection of their fundamental rights. The purpose of the study was to analyse the current legislation in the context of ensuring the protection of information about the personal data of an employee in the Republic of Kazakhstan. For this purpose, several methods were used, such as logical, formal legal comparative analysis, and dogmatic method. The norms that are regulated by the Constitution of the Republic of Kazakhstan, the Labour Code of the Republic of Kazakhstan, the Law of the Republic of Kazakhstan "On Approval of the Rules for the Collection and Processing of Personal Data" were investigated. This provided an opportunity to conduct a comparative legal analysis of the current legislative norms of Kazakhstan and European regulations. It was noted that the legal doctrine of Kazakhstan does not consolidate the fundamental principles that allow settling the issue of collecting, processing, and storing personal data of citizens. In addition, the obligation of the employer and a clear mechanism for maintaining the confidentiality of personal data of employees are not established at the state level. In this regard, recommendations were proposed to improve the current legislation. The practical significance of the results obtained lies in the possibility of using the proposed recommendations to improve the effectiveness of the mechanism for protecting information on personal data

Suggested Citation

Article's History: Received: 20.08.2024 Revised: 23.11.2024 Accepted: 23.12.2024

Syrlybayeva, F., Kassymova, X., Omarova, E., Zhussipova, B., & Nurgalieva, E. (2024). Protection of information about employee's personal data in the Republic of Kazakhstan. *Social & Legal Studios*, 7(4), 90-102. doi: 10.32518/sals4.2024.90.

*Corresponding author

of an employee in Kazakhstan, reduce the number of cases of information leakage, and bring legal norms in accordance with international standards

Keywords: privacy; human rights and freedoms; proliferation; threat; digitalisation; security

Introduction

In light of the rapid development of the digital society and digitalisation processes, the relevance of the problem of legal regulation of information security as an information resource is steadily increasing. However, an important aspect remains the achievement of an optimal balance between the changes taking place in the state and society and the individual needs of employees in ensuring the confidentiality of the personal sphere within the framework of the legal mechanism for the protection of information rights. This problem remains urgent and complex. This can be accomplished by adhering to the constitutional principle of prioritising human rights and freedoms, ensuring the inviolability of private life, personal and family secrets, and the protection of honour and dignity, which is consistent with international human and civil rights and freedoms standards. Citizens have a basic right to secrecy and the protection of their personal data (Kakeshov *et al.*, 2023). Every year in Kazakhstan, the importance of protecting citizens' personal data increases, which is associated with an increase in the likelihood of personal information leakage and the resourcefulness of fraudsters. The state and employers are obliged to provide reliable protection, properly organise activities to protect the rights of employees and avoid the risks associated with violations in the field of storage and processing of personal data (Mentukh & Shevchuk, 2023).

According to E.N. Nurgalieva and F.M. Syrlybaeva (2020), a new institution is currently being formed in Kazakh labour law – the right to information of subjects of labour law and its protection. This right includes a number of powers, such as access to information and processing of information, namely its storage, combination, transmission, dissemination or other use. Following E. Yerbolatov *et al.* (2020), a separate aspect is the right to protection of information about labour rights, which is implemented within the framework of the relationship of protection of workers' rights. Modern technologies allow employers to use personal data for their activities on a scale previously impossible. F.M. Syrlybaeva (2022) notes that in this regard, they must ensure a high level of protection of such data based on a reliable legal foundation in the field of protection of information rights of employees. The large-scale changes that are currently taking place in almost all countries are associated with the rapid development of information and communication technologies (ICT). The development of these technologies is happening so fast that all subjects of information relations have the opportunity to access and use various databases. According to S.B. Akhmetova *et al.* (2023), the process of development of the information society, despite the obvious positive results, also generates legal, moral, social and other problems and threats. In this regard, the stage of development of modern society towards information transparency requires reflection and understanding of the consequences for the future.

L.S. Asainova (2021) mentions that in the process of developing an information society, the ways of dissemination and exchange of information change, and the structure of the information space undergoes radical changes. Modern technologies, such as automatic data processing, the creation of global communication networks and the introduction of electronic management, allow collecting, processing, and distributing information with high speed and accuracy. Following B.M. Maksutov (2019), this creates serious threats to the use of personal data of citizens by authorities and individuals contrary to the interests of data subjects, and sometimes with the aim of violating their rights and legitimate interests. Technical means provide ample opportunities for collecting, storing and processing large amounts of socially significant information in various automated systems. However, these systems aimed at structuring, storing, and searching for socially significant information create the problem of leakage and other forms of illegal access to personal data, which emphasises the importance of ensuring legal protection of personal information.

N.N. Alkhamsi and S.S. Alqahtani (2024) examined the creation of a compliance framework for personal data protection laws. The researchers underlined the need of clear standards and efficient enforcement methods for ensuring that organisations follow data protection legislation. Their research emphasised the significance of connecting legislative frameworks with technology improvements in order to protect individuals' privacy rights while also encouraging responsibility among data controllers. R.S. Shahrullah *et al.* (2024) investigated Indonesia and South Korea's personal data protection legislation, focussing on how both legal frameworks uphold privacy rights. Both nations' continuous attempts to improve personal data privacy while navigating the challenges of enforcement and compliance were disclosed. By evaluating the similarities and contrasts in their approaches, the study identified crucial lessons that Kazakhstan might apply to enhance its own data protection legislation. The study underscores the idea that comprehensive legal frameworks are essential for effectively protecting privacy rights in the face of growing data collection and processing. Z. Guo *et al.* (2024) researched the evolution of personal data protection in China, focussing on the transition from a monistic to a dualistic approach in civil and criminal law. Their research demonstrates a growing realisation of the necessity for various legal approaches to manage personal data protection completely. This study emphasises the necessity of adjusting legal frameworks to developing difficulties in digital privacy, as well as the need for constant development in personal data legislation to keep up with advances in technology and social expectations.

In the Republic of Kazakhstan, as in many modern states, addressing these challenges requires the use of a wide range of executive, organisational, and technical measures and the creation of a legislative mechanism. Based on this, the purpose of the study was to examine the shortcomings the current legal doctrine of Kazakhstan in the context of ensuring the protection of employees' personal data. To achieve these goals, it was necessary to investigate the concept of "personal data", conduct a comparative legal analysis of the legislation of Kazakhstan and other acts, and identify a range of problems that reduce the effectiveness of the mechanism for protecting citizens' data.

Materials and methods

This study was carried out using various types of analysis. The functional analysis was used to investigate the protection of information about personal data of an employee in Kazakhstan, to determine its functional components, processes, and security measures. This provided an opportunity to identify which data is considered personal and requires protection, to consider potential threats to data security, and to assess the level of protection of the current information system from identified threats. The functional analysis helped to evaluate the information protection system for personal data of employees in Kazakhstan in terms of its functionality and effectiveness. The method of logical analysis was used to investigate the personal data protection system, potential vulnerabilities in the logical structure of the information system that can be used for unauthorised access or data leakage, compliance of the personal data processing system with the data protection legislation in Kazakhstan, and detection of inconsistencies.

The formal legal method provided an opportunity to study the norms regulated by the legislation on the protection of personal data. Thus, the provisions of the International Covenant on Civil and Political Rights (1996), Constitution of the Republic of Kazakhstan (1995), Law of the Republic of Kazakhstan No. 94-V "On Personal Data and their Protection" (2013), Law of the Republic of Kazakhstan No. 115-VIII "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on State Control and Statistics, Improvement of the Population Protection System, Data Management, Registration of Legal Entities and Exclusion of Excessive Legislative Regulation" (2024), Labour Code of the Republic of Kazakhstan (2015), Entrepreneurial Code of the Republic of Kazakhstan (2015), Code of the Republic of Kazakhstan "On Administrative Offences" (2014), European Social Partners Autonomous Framework Agreement on Digitalisation (2020), General Data Protection Regulation (GDPR) (2018), Order of the Minister of Digital Development, Innovation and Aerospace Industry (MDDIAI) of the Republic of Kazakhstan No. 395 "On Approval of the Rules for the Collection and Processing of Personal Data" (2023) were investigated.

The method of legal hermeneutics has been applied to analyse and interpret legislation and legal documents, including laws on personal data protection. This method helped to investigate and understand the content of laws and regulations, determine their meaning and application. In the context of studying policy on the security of personal data, the method of legal hermeneutics was used to consider in detail the text of laws, terms, definitions, and structure, to determine the meaning of key concepts used in laws, to specify the purposes of laws and their interpretation. The dogmatic method was used to review the legislation on the protection of personal data, which helped to analyse and interpret existing norms and principles, and identify the relationships between them.

The method of comparative legal analysis was used to compare the norms of the GDPR (2018) and the Law of the Republic of Kazakhstan No. 115-VIII (2024) to identify similarities and differences between them. This provided an opportunity to analyse the key terms and principles in these regulations, compare structures, formulations, and mandatory elements. Although Kazakhstan is not required to adhere to European Union standards, comparing its legislation to the GDPR gives significant insights into best practices and global trends in data protection. This comparison helps to determine how Kazakhstan's law addresses personal data privacy in a rapidly digitalising world, as well as whether it incorporates robust mechanisms found in internationally recognised regulations such as the GDPR, which is frequently cited as a benchmark for comprehensive data protection frameworks. The method of comparative legal analysis helped to investigate two key regulations and assess their impact on the practice of personal data processing in Kazakhstan. The deduction was introduced to provide characteristics about the "employee's personal data" by highlighting the key principles, features, and structure of the protection mechanism. In turn, the induction method, based on the established legislative norms, allowed characterising the mechanism for protecting personal data of an employee in Kazakhstan.

Results

Due to the increasing threat to the security of personal data, laws are being adopted in some countries that provide certain individuals with control functions in the collection, processing, and transfer of personal data to both public and private organisations. The adoption of legislative acts on the regulation of information resources in various countries has become the basis for the development of a branch of law known as information law, which includes public relations related to the legal regulation of information circulation, its creation, storage, processing and use employing communication technologies, and its protection.

The growing frequency and severity of data breaches in recent years has had a significant impact on personal data security, particularly in the United States. According to the Identity Theft Resource Center's (2024) report, the United States remains the most impacted country, with over 2,365 documented intrusions in 2023 alone. These instances, which represent the vast majority of global breaches, have exposed extremely sensitive information such as Social Security numbers, healthcare records, and financial data. Phishing attacks and ransomware were the primary causes, accounting for more than 18.5% and 10.4% of total breaches, respectively. The healthcare and banking industries were notably affected, with over 800 compromises because of the high value of medical data on the black market (101 of the latest data…, 2024).

In 2024, the situation has only gotten worse, with a number of high-profile breaches shattering people's trust in data security. A breach at Find Great People in July 2024 revealed the personal information of approximately 12,000 people, including Social Security numbers and medical records (Borelli, 2024). Similarly, the ShinyHunters organisation engineered the Ticketmaster breach in May 2024, which compromised the personal information of over 500 million individuals, making it one of the most significant breaches in recent history. This attack revealed personal identifiers and partial credit card information, fuelling concerns about massive financial theft. Furthermore, the AT&T breach in July 2024 affected call records and text message data for nearly all of its customer base (Sicurella, 2024).

In early 2024, the National Public Data breach (2024) revealed over 2.7 billion records and affected 170 million individuals. These breaches have far-reaching effects, since stolen data may be used to commit identity theft, phishing

schemes, and unauthorised financial transactions. The escalating cost of breaches also places a significant financial strain on organisations. A single mega breach may cost an average of $332 million, with 20% of breaches in the US resulting in regulatory fines surpassing $250,000 (101 of the latest data…, 2024). These instances emphasise the rising need for robust cybersecurity solutions, including multi-factor authentication, personnel training, and improved security infrastructures. With the United States highest on the number of reported breaches each year, the problem of protecting personal and organisational data remains crucial.

Kazakhstan has not been immune to the global increase in data breaches, and the country has faced growing cybersecurity issues in recent years. One of the most prominent events came in 2021, when a major breach revealed the personal information of millions of Kazakh individuals, exposing flaws in the country's digital infrastructure (Buchelnikova, 2024). This hack exposed sensitive data such as national identity numbers and personal details, raising questions about the effectiveness of cybersecurity in both the public and commercial sectors.

Data breaches in Kazakhstan have grown dramatically during 2018, indicating the country's expanding cyber threat scenario. According to JSC State Technical Service (2023), Kazakhstan saw over 223 million attempted cyberattacks in 2023, with targets ranging from government institutions to telecoms and private organisations. This is a significant increase in cyber events over prior years, especially as the country continues to digitalise its economy. Furthermore, Kazakhstan's important position in Central Asia and importance in regional commerce have resulted in a rise in cyber threats to vital infrastructure. As the country's digital economy grows, weaknesses in its cybersecurity architecture, notably in telecommunications, healthcare, and finance, have grown increasingly apparent. To counteract escalating threats, the government has emphasised the need for stronger legislative frameworks as well as modern cybersecurity technology. The government has implemented measures to improve personal data privacy, progressively matching its rules with international standards such as GDPR (Personal data protection in Kazakhstan, 2022). These reforms include requiring organisations to inform authorities of breaches and enforcing stricter standards for how personal data is maintained and used within the country. The Ministry of Digital Development, Innovations, and Aerospace Industry has been entrusted with managing these security measures, although capacity concerns remain a concern. To address these difficulties, Kazakhstan has worked to enhance its national cybersecurity policy by investing in security infrastructure, increasing citizens' digital literacy, and collaborating with foreign partners. However, as the volume of digital data increases, the dangers of data breaches remain a major issue for both individuals and organisations across the country.

The above suggests that the confidentiality of personal data is under threat. In this case, it is advisable to mention that in 2022, 31% of companies in Kazakhstan were subjected to cyber-attacks, which makes it important to consider these issues to resolve the main aspects that will strengthen the protection of personal data of employees at the legal level (Every third company…, 2023). Cyberattacks were most commonly directed at government agencies, with 133.5 million attacks on local executive bodies. In all, government entities suffered around 47.7 million assault attempts, emphasising the importance of enhanced cybersecurity measures in the public sector (JSC State Technical Service, 2023). This is a huge increase over prior years, when cyberattacks were fewer and less sophisticated.

Citizens' information rights are enshrined in the International Covenant on Civil and Political Rights (1996), which is binding on almost all countries of the world, including Kazakhstan; articles 17-21 of this Covenant. Information rights are also contained in articles 10-39 of the Constitution of the Republic of Kazakhstan (1995), which, although they do not directly regulate the issues of ensuring the protection of personal information rights, nevertheless serve as basic provisions. In 2013, Kazakhstan adopted the Law of the Republic of Kazakhstan No. 94-V "On Personal Data and their Protection" (2013), which for the first time took into account international standards. The main priority of this law is to ensure the protection of human and civil rights and freedoms in the collection and processing of personal data. It also regulates public relations in the field of personal data and establishes the legal basis for their protection. Additional changes were made with the adoption of Law of the Republic of Kazakhstan No. 115-VIII (2024). The revisions were intended to strengthen the present legislative framework, particularly in terms of governmental control, data management, and population protection. The changes aimed to increase government oversight systems for personal data processing and guarantee that enterprises that handle personal data follow amended regulations. These reforms indicate Kazakhstan's commitment to modernising its regulatory framework in response to the growing complexity of data security in the digital age.

It is worth noting that the provisions of this law are not reflected in the current Labour Code of the Republic of Kazakhstan (2015), where there are no articles on personal data and their protection. The Labour Code only mentions the employee's right to protect the data stored by the employer. These references to personal data legislation do not sufficiently solve the problem of information protection within the framework of employment relations, which, of course, has its own characteristics. The employer's obligation to protect the employee's information rights includes the protection of the employee's personal data exclusively in the context of an employment relationship, such as information about the employee, his/her professional qualifications, business and professional qualities, but should in no way affect personal and family life (Rieger *et al.*, 2019). To prevent unjustified expansion of information about an employee in the Labour Code, it is necessary to establish a list of information that is prohibited from being required from an employee.

The problems of personal data leakage indicate the existence of a number of problems. Each government agency that has databases must independently be responsible for storing personal data in its databases and comply with the rules for the use and secrecy of information stored there (Hina *et al.*, 2019). In addition to the problem of leakage of personal information, important aspects include liability for violations of relevant regulations, including the dismissal of the head of the department responsible for the collection and storage of personal data. Currently, there are no statistics on personal data protection in Kazakhstan. Based on this, it is necessary to develop a culture of personal data protection, especially among employers, including reporting information violations to the employee himself, which will help

establish trusting relationships and assign responsibility for the collection, processing, and storage of personal data; ensure the confidentiality of information about the employee, which consists in restricting access to this data. Protecting an employee's information data is a technical issue, whereas data privacy is a legal issue. Many information privacy protection protocols are still vulnerable to authorised persons to whom this information is available. It is also important to ensure the technological capabilities of the subjects for cooperation. With regard to the protection of information data, it is necessary to establish a range of entities that have access to and control the safety of collecting, processing and storing information about an employee obtained using various devices, such as video surveillance (Yakymenko, 2023).

Government agencies and organisations own and manage various informatisation facilities and databases, as they provide electronic services, which gives them access to personal data of citizens. In order for their activities and technical infrastructure to always meet the requirements of information security and be maximally protected from possible hacker attacks and internal threats, there is an authorised body in Kazakhstan responsible for monitoring information security, namely MDDIAI. According to the Entrepreneurial Code of the Republic of Kazakhstan (2015), this authorised body conducts preventive control and unscheduled inspections that help to identify inconsistencies with information security requirements in the work of government agencies and organisations. In case of detection of the facts of illegal collection or leakage of personal data, and violations of the rules for the use of electronic digital signatures, citizens have the right to contact the authorised body in any convenient way to register a complaint (for example, electronically, by mail, through the portal of "Electronic Government" or another way). According to such appeals, the authorised body has the right to start an inspection against the violator, initiate an administrative case and bring him to justice in accordance with the Code of the Republic of Kazakhstan "On Administrative Offences" (2014).

Despite the presence of specialised agencies controlling supervision and other institutions, it is important to note that virtually all government agencies, their committees, departments and departments work with at least one database. The protection of employees' information rights should be an essential link that promotes harmonious relations among state bodies and between these entities and society. This strategy intends to improve trust and communication, two critical components of a digital society. The Law of the Republic of Kazakhstan No. 94-V (2013) provides the foundation for this societal revolution. It should be mentioned that the technical requirements to secure information containing personal data apply only to public authorities. Significant revisions have been made to Article 27, which now clearly specifies the roles of central and local government entities. These changes include a systematic structure for developing and approving legal acts relating to personal data protection, handling appeals from individuals and businesses, and enforcing compliance. Local executive bodies, in particular, are granted more authority to ensure that personal data is legitimately managed within their administrative zones, including the capacity to demand the correction, blocking, or deletion of unauthorised or untrustworthy data. This demonstrates Kazakhstan's commitment to both central control and local enforcement of personal data legislation.

Monitoring the application of the law on personal data protection and monitoring compliance with the requirements for their protection are becoming the main aspects of work in the field of personal data protection (Protection of personal information, 2023). Nevertheless, to date, the existing practice does not contribute to solving systemic problems, since it postpones the solution of the most important tasks to a later date, including personnel training, the creation of a legal and information culture, and above all in government agencies. It is important to note that dismissal (for example, for improper storage or leakage of information) cannot remain the only mechanism of punishment for violation of the law, as it requires the development of clear mechanisms for accountability. Since personal data is subject to protection, and it is the state that acts as the guarantor of this protection, all those involved in the protection of personal data must comply with established technical and legal standards (Custers *et al.*, 2019). The Law of the Republic of Kazakhstan dated No. 115-VIII (2024) aimed at improving state monitoring and compliance, notably by altering Article 27 of Law of the Republic of Kazakhstan No. 94-V "On Personal Data and their Protection" (2013). This offers both central and local executive authorities clearer mandates for enforcing personal data privacy legislation, handling appeals, and penalising offenders. These amendments attempt to get past systemic enforcement deficiencies by delegating additional authority to national and regional agencies to take prompt and decisive action to resolve breaches and other infractions.

The digital transformation in labour relations brings significant benefits to both employers and employees. They include new employment opportunities, increased productivity, improved working conditions, the introduction of new methods of work organisation, and improvement of the quality of services provided (Aloisi & Gramano, 2019). Thus, with proper organisation and protection of information rights in the field of labour relations, this can lead to increased employment and job retention. The legislation of Kazakhstan does not contain an exhaustive list of public personal data and specific legal norms governing the collection and processing of such data. It is important for employers to obtain the consent of employees in advance for the processing of such data, since the purposes of using personal data that have become publicly available may not coincide with the goals stated by the organisation when collecting and processing personal data. The amendments due to Law of the Republic of Kazakhstan dated No. 115-VIII (2024) contribute to this area by enhancing the legal framework governing the collection and utilisation of employee data. The reforms help in this area by strengthening the legal framework governing the collection and utilisation of employee data. They impose stricter monitoring by state bodies, as seen by modifications to Article 27 of Law of the Republic of Kazakhstan No. 94-V (2013), which entrust local executive bodies with state responsibility over compliance with personal data protection rules, particularly those affecting private commercial companies. This guarantees that enterprises processing employee data follow established legal rules, so contributing to the protection of employees' rights as labour practices become more digital.

The authorisation and withdrawal of consent for employee personal data collecting and processing requires adherence to a key principle: the data subject's only right to offer such consent. Current national regulatory frameworks do not allow for transfer of this ability to third parties

through proxy or power of attorney processes. The modifications made by the Law of the Republic of Kazakhstan No. 115-VIII (2024), reinforce this by eliminating any option for third-party permission via power of attorney and instead focussing on expanding local and state authorities' authority over personal data processing. The amendments strengthen local executive bodies' responsibilities by assigning them the oversight of personal data processing issues within their jurisdiction, including ensuring compliance with data protection laws in cases were legal representatives, rather than third-party attorneys, act on behalf of individuals. These revisions emphasise the importance of personal data owners or their legal representatives being the only ones able to offer or withdraw consent. This right belongs only to a legal representative, that is, a person who can act on behalf of an individual in state bodies, since the protected person is not able to exercise his or her rights and duties directly due to age or physical limitations. That is, employers should take this circumstance into account, and legislation should provide for the possibility of giving consent to the processing of personal data by an employee through a trusted person.

As indicated in the Labour Code of the Republic of Kazakhstan (2015), the general requirements for processing employee personal data are regulated by the norms that define the obligations of the employer to collect, process, and protect personal data. Based on this, each employer must establish a clear procedure for collecting, processing, and protecting personal data by adopting an internal document and familiarising all employees with it. With Law of the Republic of Kazakhstan No. 115-VIII (2024), employers' duties in managing personal data are indirectly enhanced by the expanded enforcement powers granted to state entities under Article 27 of Law of the Republic of Kazakhstan No. 94-V (2013). The legislation requires local executive authorities to monitor private commercial organisations' compliance with data protection rules in their area. This underlines the need of organisations to strictly follow internal data handling practices and establishing explicit data protection policies. Refusal to comply may result in local authorities implementing enforcement actions, such as penalties for non-compliance, emphasising the significance of ensuring that only authorised individuals have access to employee data.

The employer must restrict access to personal data of employees and appoint those responsible for their processing. Data processors should only access the information necessary for fulfilling their official responsibilities, while maintaining confidentiality. A large amount of data is accumulated when doing work, but often managing this data is not a priority. Issues related to the legal aspects of data collection, access, and sharing remain unresolved. This affects the confidentiality of information about employees, their mobility in their careers and the quality of the work performed. Collective rights must also be protected, as regulators usually pay attention to protecting the rights of individuals or protected groups, such as those of a particular gender, age, ethnicity, or sexual orientation. While Law of the Republic of Kazakhstan No. 115-VIII (2024) does not explicitly address collective rights or provide extra protections for sensitive personal data like as political beliefs or ethnicity, it does bring a more organised approach to data management. Local governments now have the right to order organisations to clarify, prohibit, or remove untrustworthy or illegally obtained material. This helps to protect individuals' data in circumstances when it is unlawfully managed, but it does not currently provide collective rights protections. Additional legislative efforts may be necessary to close this gap. This is important, but not enough to ensure real freedom of action for both employees and employers and their representatives.

COVID-19 has brought new data sources to the work environment through the collection of health information and remote work (Podoprigora *et al.*, 2019). The digital revolution has significantly transformed the global professional landscape, resulting in a notable increase in remote work. Data indicates that the proportion of employees working remotely rose from 20% in 2020 to 28% by 2023. Within this context, the technology sector exhibited the highest prevalence of remote work, with 67% of its workforce primarily operating from home (Sherif, 2024). Often, employee data is collected during hiring and during work through communication tools, interfaces, and sensors. This employee-related data can bring value to employers, especially in terms of improving productivity. However, the capabilities of employees are often limited due to complex technical aspects, lack of transparency and lack of means to protect their individual and collective rights to personal and collective data.

European Social Partners Autonomous Framework Agreement on Digitalisation (2020) entitles employee representatives to participate in issues related to consent, confidentiality and monitoring, following the GDPR (2018). However, GDPR applies only to personal data, and the assumed and observed data that is often collected in the workplace does not always fall under this definition. Existing legal frameworks lack a specific definition of "confidential data". This uncertainty applies to a wide range of sensitive information, including racial or ethnic identifiers, political views, trade union connections, religious beliefs, health-related data, sexual orientation, and genetic or biometric markers. The lack of specific legislative definitions for various data types complicates their legal categorisation and protection. Employers can use such data in an employment relationship without significant restrictions. Law of the Republic of Kazakhstan No. 115-VIII (2024) reinforces this framework by increasing governmental control over the processing of personal data. Specifically, the new Article 27 gives state agencies more ability to enforce compliance with data privacy legislation. It allows them to impose sanctions on organisations that do not adopt sufficient internal controls, such as those governing employee data access and processing. This strives to guarantee that personal data handling inside organisations meets the appropriate requirements. Technologies are constantly evolving, new identification methods are emerging, and the employer must monitor such innovations. It is also necessary to legislatively regulate the procedures for the collection and processing of personal data of employees not only at the stage of their use, but also at the stage of development.

In comparison with the principle of legality in the Law of Kazakhstan, the GDPR (2018) establishes a more specific and specific nature of the principle of legality, fairness, and transparency. It not only requires compliance with the law when collecting and processing data, but is also one of the fundamental concepts and a key condition for the protection of personal data. The legality of the processing of personal data in the GDPR is supported by the requirement to obtain consent from an individual. Consent must be free, specific, informed and unambiguous, and in its absence, data collection

and processing are considered illegal, except in cases provided for by law. In addition, Articles 13 and 14 of the GDPR establish clear requirements for the information that the data controller is obliged to provide to the data subject at the time of collection of his/her personal data. Mandatory information includes the contact details of the person responsible for the protection of personal data, the purpose of data processing, the conditions for transferring data to third parties, indicating measures to protect them, the terms of data storage, an indication of automated data processing and other details. The alteration to Paragraph 2 of Article 17 of Law of the Republic of Kazakhstan No. 94-V "On Personal Data and their Protection" (2013) through Law of the Republic of Kazakhstan No. 115-VIII (2024) eliminates the need for the authorised data management authority to approve certain data processing operations. This simplifies the procedure but adds no additional particular responsibilities to alert data subjects about its collection, use, or transfer of their personal information. In comparison, the GDPR (2018) sets tougher standards, including the need that permission be free, explicit, informed, and clear (GDPR, Article 6). Consent must be sought prior to data collection, and data controllers are expected to give persons with full information about the purpose of data processing, storage durations, and potential data sharing with third parties (GDPR Articles 6, 13, and 14). The changes to Kazakhstan's law do not address the unique concerns of transparency and informed consent.

The modified Article 27 Law of the Republic of Kazakhstan No. 115-VIII (2024) empowers state and municipal executive authorities to design and adopt normative legal actions, respond to data subjects' concerns, and hold offenders responsible. Furthermore, local organisations are responsible for assessing individual appeals against the processing of their personal data and ensuring that private commercial firms within their jurisdictions comply with data protection regulations. These municipal organisations also have the authority to order the blocking, removal, or clarification of unlawfully obtained or inaccurate data. While this improves state monitoring and enforcement, it does not create specific duties for data controllers to proactively notify data subjects before collecting personal information, creating a gap in comparison to the GDPR's more stringent requirements.

The GDPR (2018) relies on the principles of legality, fairness, and transparency, with Articles 13 and 14 requiring controllers to provide clear, detailed information at the time of data collection, including the controller's identity, the purpose of the data collection, data transfer conditions, retention periods, and whether automated decision-making is involved. This guarantees that consent is fully informed and voluntary. The Kazakh revisions, however, do not include such clauses, implying that, while there is better enforcement, the legislation does not completely address the concepts of transparency and individual rights to the same extent as the GDPR.

The data controller must inform the data subject of his or her rights, including the right to withdraw consent, the right to protection in the state body for the protection of personal data, the right to access personal data, the right to correction, the right to deletion. According to Article 12 of the GDPR (2018), the controller and the operator are obliged to provide information to the data subject in a clear, direct, and understandable form, using simple and understandable language. In comparison with the GDPR, the current Law of Kazakhstan No. 115-VIII (2024) does not contain obligations for database owners and operators regarding the collection of personal data, does not establish important requirements for informing data subjects before obtaining consent to the processing of personal data, and does not provide clear requirements regarding the freedom of consent and the level of awareness of data subjects. Law of the Republic of Kazakhstan No. 115-VIII (2024) primarily clarifies the roles of state and local executive bodies in overseeing compliance with data protection laws, handling complaints, and enforcing actions against violations. However, it does not introduce specific obligations for database owners and operators to inform data subjects about personal data collection and use before obtaining consent. The law states that state bodies "take measures to bring persons who have committed violations of the legislation... to responsibility" and that local executive bodies "exercise state control over compliance with the legislation... in relation to private business entities" (Article 27.1(3) and 27.2(2)). These provisions enhance the government's ability to enforce compliance but do not explicitly require database owners to provide data subjects with detailed information about the purpose of data collection or data retention periods.

Law of the Republic of Kazakhstan No. 115-VIII (2024) does not introduce detailed requirements for ensuring that data subjects are fully informed about the processing of their data. While local bodies are given the power to demand the clarification, blocking, or destruction of unreliable or illegally obtained personal data (Article 27.2(4)), this does not extend to establishing clear requirements for transparency before consent is given. As a result, the law still lacks provisions that mandate database operators to provide data subjects with clear, informed, and unambiguous information regarding the collection and processing of personal data. Although the amendments improve enforcement capabilities, they do not address the issue of ensuring that consent is freely given and informed. The GDPR (2018) requires that consent be "free, specific, informed, and unambiguous", but these detailed standards are not reflected in the 2024 amendments. The Kazakh law does not provide requirements similar to the GDPR's Articles 13 and 14, which set forth the need to inform data subjects about the purpose of data collection, data transfer conditions, and data retention periods.

In accordance with Order of the MDDIAI of the Republic of Kazakhstan No. 395 "On Approval of the Rules for the Collection and Processing of Personal Data" (2023), it is determined which data should be included in the consent, how it should be provided, and even set its validity period. The revisions to this order emphasise the need of obtaining explicit agreement from the data subject or their legal representative before collecting personal information. They also outline the procedures for acquiring this permission through both government and non-governmental agencies. The updated regulations limit data collection to what is deemed necessary and adequate, as specified in an authorised list of personal data. Furthermore, any distribution of data in publicly available sources requires the subject's agreement, fostering a higher level of transparency. The requirements demand that all personal data be stored within Kazakhstan, resulting in stricter controls on cross-border data transfers. This integrates Kazakhstan's system with international data protection standards, ensuring that personal information is managed more securely and accountable.

Order of the MDDIAI of the Republic of Kazakhstan No. 395 "On Approval of the Rules for the Collection and Processing of Personal Data" (2023) allows that database owners and operators can request other information about the data subject with the consent of the data subject, but the authorised body stressed that the list of these data should be exhaustive. The intent is to grant transparency and restrictions in data processing. The order's need for an exhaustive list of data that can be sought from data subjects seeks to avoid unnecessary or excessive data collecting, which could lead to privacy violations. This guarantees that data controllers and processors are open about the categories of personal information they require and collect only the least amount of data required for the indicated purpose, in accordance with the concept of data minimisation. A comprehensive list also protects the data subject by specifying how the information will be used, avoiding misuse or overreach of data processing beyond the initial consent. It also adheres to international data protection regulations such as the GDPR (2018), which emphasises transparency and restricts collecting data to what is required for processing purposes.

The widespread use of advanced ICT and the intensive analysis of personal data in both commercial and public sectors necessitate a thorough revision of existing ethical and legal principles governing data protection. Regulatory principles must be resilient to rapid technological advancements and adaptable to new innovations. Specifically, the GDPR (2018) in Europe provides a model framework. Its foundational principles, such as data minimization (Article 5), and accountability (Article 24), are designed to ensure lawful and transparent processing of personal data. The implementation of such principles into Kazakhstan's legislation could strengthen the protection of personal integrity and privacy. To improve the regulatory framework in Kazakhstan the following is proposed.

The existing legislative framework of the Republic of Kazakhstan does not sufficiently address the principles of transparency and accountability. Incorporating provisions similar to Articles 13 and 14 of the GDPR is advised, which require data controllers to provide detailed information to data subjects regarding the purpose of data collection, the retention period, and the right to access their data. This will increase transparency and ensure data subjects are fully informed.

The existing Article 16 of the Republic of Kazakhstan No. 115-VIII (2024) on cross-border data transfer should be amended to specify stricter controls, similar to Article 45 of the GDPR (2018), which requires an adequacy decision before data can be transferred to a third country. This ensures that personal data transferred outside Kazakhstan will be handled with the same level of protection as within the country.

The principle of accountability is recommended to be adopted as laid out in Article 24 of the GDPR (2018) is recommended. Data controllers in Kazakhstan should be legally obligated to implement suitable technical protocols and organisational measures to facilitate adherence to data protection regulations. This can be achieved by mandating the appointment of data protection officers in public and private organizations that handle large-scale personal data. To ensure these legislative amendments translate into practical improvements, the following measures are proposed:

1. Following the regulatory framework established by Article 35 of the GDPR (2018), it is proposed that entities operating in Kazakhstan be required to conduct Data Protection Impact Assessments (DPIAs) for high-risk data processing operations. These DPIAs, required by GDPR Article 35, have proven effective as analytical tools for identifying and mitigating privacy-related vulnerabilities in data processing procedures. Implementing such a requirement will bring Kazakhstan's data protection policies in line with internationally recognised norms while also strengthening the data governance system.

2. A study by M. Friedewald *et al.* (2022) reports that integrating DPIAs into project management early on helps organisations proactively address privacy concerns before systems are implemented. The study found that DPIAs, when executed thoroughly, reduced high-risk data processing and facilitated compliance with privacy by design principles. These practices are particularly relevant for high-risk sectors such as health and IoT services, where personal data is processed extensively.

3. Empirical studies show that public awareness regarding data protection significantly enhances the effectiveness of laws. Special Eurobarometer 487a (2019) found that 73% of EU citizens were aware of at least one of their rights under the GDPR. This increased public awareness correlates with a higher demand for transparency from businesses regarding how personal data is collected and used. The survey highlights the positive impact of robust data protection regulations and public education campaigns in fostering trust between individuals and organisations. Kazakhstan could replicate this success through public campaigns that educate individuals about their data rights and the obligations of businesses and state institutions under the new regulations.

4. Integrating ICT and digital governance can support data protection while maintaining efficient public services. Estonia and Finland have successfully integrated ICT and digital governance into their national frameworks, ensuring efficient public services while maintaining robust data protection. Estonia's e-Governance model, for example, showcases how digital public services can be securely managed with a strong focus on data privacy. A study by R. Adeodato and S. Pournouri (2020) shows how Estonia's e-Estonia program, in conjunction with legal frameworks, has enhanced both service efficiency and data protection. Kazakhstan could consider a similar digital transformation strategy, integrating data protection into the broader framework of e-governance initiatives to safeguard personal data more effectively.

Kazakhstan may develop a strong and future-proof regulatory framework by aligning its data protection legislation with globally best practices, such as those outlined in the GDPR, and implementing both legal and practical suggestions based on proven cases and empirical data. This will not only preserve individuals' private rights, but will also increase confidence in digital services, resulting in a safer digital society.

Discussion

The amendments with Law of the Republic of Kazakhstan No. 115-VIII (2024) on personal data and their protection make significant changes to the oversight and enforcement of data protection laws but fall short of addressing key GDPR (2018) requirements such as transparency and informed consent. Specifically, while the new amendments (particularly the revised Article 27) clarify the roles of central and local government bodies in addressing complaints,

monitoring compliance, and enforcing data protection violations, they do not impose specific obligations on database operators to notify data subjects before collecting personal data. This contrasts with the GDPR's strict transparency requirements, stated in Articles 13 and 14, which require data controllers to publish extensive information about the purpose of data processing, data retention periods, and restrictions for transferring personal data to third parties.

The law's solidified enforcement measures enhance state control over compliance by allowing local executive bodies to order the corrections, blockage, or elimination of unlawfully obtained or erroneous data (Diegtiar *et al.*, 2023). However, these modifications do not create additional procedures to ensure that data subjects are adequately informed prior to data collection, which remains a significant gap. The lack of specific standards for freedom of consent and data subject knowledge highlights the distinction between Kazakhstan's framework and the GDPR (2018). As a result, while the revisions strengthen governmental monitoring, they do not achieve the degree of openness and accountability required by international standards, notably those established by the GDPR. The study stresses the need for Kazakhstan to tighten its data protection regulations by implementing GDPR concepts such as openness, data minimisation, and accountability. Specific ideas include modifying the legislation to compel data controllers to give data subjects with full information about the purpose of data collection and cross-border data transfers, as well as employing data protection officers in organisations that handle substantial amounts of data. Furthermore, completing DPIAs for high-risk operations and raising public knowledge of data rights are advised strategies for ensuring strong data security. Integrating ICT and digital governance, inspired by successful systems in Estonia and Finland, is also proposed to improve data security and service efficiency (Semeniuk & Horbach-Kudria, 2024).

According to T.T. Ke and K. Sudhir (2022), it is quite important to distinguish between confidential and secret information about a person. It is worth adding that in this case, additional and significant difficulties arise due to the presence of several types of "secrets" in the legislation, including various legal regimes that include the term "secret", such as banking, medical, law. C. Chang *et al.* (2019) investigated the automated extraction of privacy policies under the GDPR, demonstrating how technological developments might improve regulatory compliance. In contrast, Kazakhstan's legal structure lacks such automatic procedures, allowing for oversight gaps and limited transparency. D. McGraw and K.D. Mandl (2021) write that currently, the main difference between confidential information about an individual and secret information is that the regulation of the legal status of confidential information is based on the principle of voluntariness, while restricting access to secret information is mandatory and established by law. Based on this, it can be concluded that the provision of confidential information is always the implementation of the right of a certain subject of information relations, and when access to confidential information is restricted, it is the fulfilment of obligations provided for by relevant legislation.

V.B. Kumar *et al.* (2020) noted that confidential information is considered to be information to which access is restricted by the subject of personal data, while secret information is considered to be data that is subject to secrecy in accordance with the law. It should be added that confidential information includes aspects such as information about the private life of a citizen, such as facts, events and circumstances, or personal data that allow the identification of a citizen, with the exception of information that is subject to publication in the media in accordance with established rules. V.B. Kumar *et al.* (2020) examined the automatic extraction of opt-out statements, emphasising how modern technology may assure compliance with data privacy rules. The absence of such procedures in Kazakhstan's legislative framework demonstrates a huge technology gap that hinders effective data management. Both current research and international studies agree on the significance of increasing automation and transparency in order to achieve GDPR-level protection while managing personal data.

R.N. Zaeem and K.S. Barber (2020) write that personal data includes information related to a specific individual, such as last name, first name, patronymic, temporal and geographic markers of origin, residential information, relational status, socioeconomic indicators, education, profession, and income. Examples of personal data include passport data, information about marital status, information about education, taxpayer ID number, data from the insurance certificate of state pension insurance and health insurance, information about employment, information about social and property status, and income data. In turn, according to H. Li *et al.* (2019), various data are also collected in medical institutions for the treatment of a patient, including test results and information about benefits, health insurance, and previous treatments. Confidentiality of personal data is mandatory for all services and organisations that have access to this data, such as government agencies, legal entities, and individuals who organise the processing of personal data of employees of the enterprise.

N. Truong *et al.* (2021) note that the personal data information system is a system that includes a set of personal data stored in a database, including technical means that allow automating their processing. The processing of personal data includes various operations that manipulate, manage, and transform individual-specific information. M. Di Martino *et al.* (2019) note that when processing personal data, the operator must take all necessary organisational and technical measures to protect this data from unauthorised access, destruction, modification, blocking, copying, and dissemination. The operator creates a commission that assesses data and assigns a security level to the personal data information system. This level determines the processing category, volume, information resource type, processing modes, and user access rights differentiation, ensuring the security of the enterprise security system. Also, M. Di Martino *et al.* (2019) identified possible flaws in the GDPR's right of access and demonstrate how they might be abused to leak personal information. This study emphasises the importance of stringent enforcement methods, a worry that current research on Kazakhstan also emphasises, given the shortcomings in its implementation of personal data regulations. In both circumstances, the lack of robust monitoring and thorough protection measures makes personal information vulnerable to exploitation.

In the legal regulation of the turnover of personal data, two main directions arise, which provide for the specific features of the legal regime of such data. First of all, according to L. Bradford *et al.* (2020), this includes ensuring the confidentiality of personal data in the process of their collection and processing in information systems, when a person

interacts with government agencies and other organisations in the course of his activities. Secondly, it includes ensuring the confidentiality of personal data through the interaction of an individual with the media. Each individual uses his/her personal data to exercise his/her rights and obligations by participating in public relations regulated by legal norms and providing personal data for legal circulation. This leads to the accumulation of personal data, which involves the owners of databases containing personal data and the operators of such databases. Despite the fact that careful legal regulation of the mechanism for ensuring the confidentiality of personal data is a necessary condition for their legal turnover, it is fraught with certain difficulties. M. Finck and F. Pallas (2020) mention that maintaining the confidentiality of personal data requires organisational, technical, financial, and economic costs. It is worth agreeing with the above, as this creates difficulties for some personal data operators, who cannot always properly comply with the legislation due to redundant legal provisions.

This study identifies substantial deficiencies in Kazakhstan's data protection regime, notably in transparency, accountability, and enforcement, in comparison to international norms such as the GDPR. The findings indicate that, while legal amendments like Law of the Republic of Kazakhstan No. 115-VIII (2024) have enhanced state control, they fall short of completely informing data subjects and implementing particular consent methods. This study emphasises the need for increased transparency in collecting data and stricter enforcement of data protection regulations, as well as practical recommendations for policy reforms and the adoption of GDPR-aligned measures to improve data security and protect personal information in Kazakhstan.

Conclusions

The rising appearance of data breaches, along with rapid improvements in ICT, has required updates to data protection regulations across the world, including in Kazakhstan. The 2024 modifications to Kazakhstan's Law No. 94-V "On Personal Data and Their Protection" aimed to improve the legal framework, notably by defining the obligations of state and local executive authorities in data collecting and processing. However, a careful comparison of the GDPR with Kazakhstan's amended law finds that, while the 2024 modifications improve governance, they fall short of GDPR requirements in numerous critical areas.

One of the most significant changes between the 2013 and 2024 laws is the expansion of governmental monitoring and the implementation of more specific enforcement authorities to oversee data protection. For example, Article 27 of the 2024 legislation outlines state authorities' obligations in producing normative legislative actions, resolving data protection violations, and monitoring compliance at the local level. The amendments also required local governments to address data subject appeals and implement stronger compliance measures. However, these changes prioritise administrative enforcement above enhancing openness and data subjects' rights, which are key to the GDPR.

The new law lacks key GDPR provisions, such as the requirement for data subjects' free, specific, informed, and unambiguous consent (GDPR Article 6), as well as the obligation to provide data subjects with detailed pre-collection information about the purpose of data processing, retention periods, and data transfer conditions (GDPR Articles 13 and 14). Accountability provisions, such as those included in GDPR Article 24, which require data controllers to establish organisational and technological measures for compliance, are lacking in Kazakhstan's legislation. The law does not address the need for greater transparency in employment-related data collecting, which allows sensitive information such as political opinions, ethnicity, or trade union membership to be gathered without specific constraints. Further reforms are necessary to fully secure the privacy rights of employees in Kazakhstan's digital economy.

The Law No. 115-VIII outlines broad requirements for database owners and operators regarding the collecting of personal data, which differs from Law No. 94-V. However, it falls short of establishing precise obligations for informing data subjects prior to gaining consent, as well as defined rules for data subjects' freedom of consent and degree of awareness. This contrasts with international frameworks such as the GDPR, which have more thorough laws in these areas. Future research should focus on developing more comprehensive frameworks that incorporate technological advancements, such as automated data protection systems, as well as assessing the efficacy of newly implemented regulations in reducing breaches and increasing public trust in data security.

Acknowledgements

None.

Conflict of interest

None.

References

[1] 101 of the latest data breach statistics for 2024. (2024). Retrieved from https://secureframe.com/blog/data-breach-statistics

[2] Adeodato, R., & Pournouri, S. (2020). Secure implementation of e-governance: A case study about Estonia. In *Cyber defence in the age of AI, smart societies and augmented humanity. Advanced sciences and technologies for security applications* (pp. 397-429). Cham: Springer. doi: 10.1007/978-3-030-35746-7_18.

[3] Akhmetova, S.B., Ibrayeva, A.S., Baimakhanova, D.M., Baikenzheyev, A.S., & Tursynkulova, D.A. (2023). Principles of protection of personal data: Comparative analysis of national and foreign legislation. *Journal of Actual Problems of Jurisprudence*, 106(2) 33-46. doi: 10.26577/JAPJ.2023.v106.i2.04.

[4] Alkhamsi, N.N., & Alqahtani, S.S. (2024). Compliance framework for personal data protection law standards. *International Journal of Advanced Computer Science and Applications*, 15(7), 512-526. doi: 10.14569/IJACSA.2024.0150751.

[5] Aloisi, A., & Gramano, E. (2019). Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context. *Comparative Labor Law & Policy Journal*, 41(1), 95-121.

[6] Asainova, L.S. (2021). *Protection of personal data in the context of the use of biometric authentication technologies*. Astana: Maqsut Narikbayev University.

[7] Borelli, S. (2024). *Find great people data breach investigation*. Retrieved from http://surl.li/gsjjkd.

[8] Bradford, L., Aboy, M., & Liddell, K. (2020). COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*, 7(1), article number lsaa034. doi: 10.1093/jlb/lsaa034.

[9] Buchelnikova, V. (2024). *Leakage of personal data: How information about Kazakhstani citizens is lost and what are the risks?* Retrieved from https://factcheck.kz/analitika/utechka-personalnyh-dannyh-kak-teryayut-svedeniya-o-kazahstantsah-i-chem-eto-grozit/.

[10] Chang, C., Li, H., Zhang, Y., Du, S., Cao, H., & Zhu, H. (2019). Automated and personalized privacy policy extraction under GDPR consideration. In *14th international conference on wireless algorithms, systems, and applications* (pp. 43-54). Cham: Springer.

[11] Code of the Republic of Kazakhstan "On Administrative Offences". (2014, July). Retrieved from https://online.zakon.kz/Document/?doc_id=31577399.

[12] Constitution of the Republic of Kazakhstan. (1995, August). Retrieved from https://online.zakon.kz/Document/?doc_id=1005029.

[13] Custers, B., Sears, A.M., Dechesne, F., Georgieva, I., Tani, T., & Van der Hof, S. (2019). *EU personal data protection in policy and practice*. Hague: T.M.C. Asser Press. doi: 10.1007/978-94-6265-282-8.

[14] Di Martino, M., Robyns, P., Weyts, W., Quax, P., Lamotte, W., & Andries, K. (2019). Personal information leakage by abusing the GDPR right of access. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)* (pp. 371-385). Santa Clara, CA: USENIX Association.

[15] Diegtiar, O.A., Kravchenko, T.A., Yevmieshkina, O.L., Sych, T.V., & Linetska, Y.M. (2023). Optimisation of information and communication systems of local government. *Electronic Government*, 19(6), 734-746. doi: 10.1504/EG.2023.134019.

[16] Entrepreneurial Code of the Republic of Kazakhstan. (2015, October). Retrieved from https://adilet.zan.kz/rus/docs/K1500000375.

[17] European Social Partners Autonomous Framework Agreement on Digitalisation. (2020). Retrieved from https://www.etuc.org/system/files/document/file2020-06/Final%2022%2006%2020_Agreement%20on%20Digitalisation%202020.pdf.

[18] Every third company in Kazakhstan has experienced cyberattacks. (2023). Retrieved from https://bluescreen.kz/news/13148/kazhdaia-trietia-kompaniia-v-kazakhstanie-stalkivalas-s-kibieratakami.

[19] Finck, M., & Pallas, F. (2020). They who must not be identified – Distinguishing personal from non-personal data under the GDPR. *Max Planck Institute for Innovation and Competition Research Paper*, 19(14). doi: 10.2139/ssrn.3462948.

[20] Friedewald, M., Schiering, I., Martin, N., & Hallinan, D. (2022). Data protection impact assessments in practice. In *Computer security. ESORICS 2021 international workshops* (pp. 424-443). Cham: Springer. doi: 10.1007/978-3-030-95484-0_25.

[21] General Data Protection Regulation (GDPR). (2018, May). Retrieved from https://gdpr-info.eu/.

[22] Guo, Z., Hao, J., & Kennedy, L. (2024). Protection path of personal data and privacy in China: Moving from monism to dualism in civil law and then in criminal law. *Computer Law & Security Review*, 52, article number 105928. doi: 10.1016/j.clsr.2023.105928.

[23] Hina, S., Selvam, D.D.D.P., & Lowry, P.B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behaviour in higher education institutions in the developing world. *Computers & Security*, 87, article number 101594. doi: 10.1016/j.cose.2019.101594.

[24] Identity Theft Resource Centre. (2024). *2023 data breach report*. Retrieved from https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.

[25] International Covenant on Civil and Political Rights. (1996, December). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[26] JSC State Technical Service. (2023). *Digital shield: 2023 review in cybersecurity*. Retrieved from https://sts.kz/wp-content/uploads/2024/01/kiberdajdzhest-2023.pdf.

[27] Kakeshov, B.D., Kanybekova, B.K., Seidakmatov, N.A., Zheenalieva, A.O., & Kokoeva, A.M. (2023). Political and legal aspects of criminal and administrative responsibility for information security offences in the context of national security of the Kyrgyz Republic. *Economic Affairs (New Delhi)*, 68, 987-993. doi: 10.46852/0424-2513.2s.2023.48.

[28] Ke, T.T., & Sudhir, K. (2022). Privacy rights and data security: GDPR and personal data markets. *Management Science*, 69(8), 4389-4412. doi: 10.1287/mnsc.2022.4614.

[29] Kumar, V.B., Iyengar, R., Nisal, N., Feng, Y., Habib, H., Story, P., Cherivirala, S., Hagan, M., Cranor, L., Wilson, S., Schaub, F., & Sadeh, N. (2020). Finding a choice in a haystack: Automatic extraction of opt-out statements from privacy policy text. In *Proceedings of the web conference* (pp. 1943-1954). New York: Association for Computing Machinery. doi: 10.1145/3366423.3380262.

[30] Labour Code of the Republic of Kazakhstan. (2015, November). Retrieved from https://online.zakon.kz/Document/?doc_id=38910832.

[31] Law of the Republic of Kazakhstan No. 115-VIII "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on State Control and Statistics, Improvement of the Population Protection System, Data Management, Registration of Legal Entities and Exclusion of Excessive Legislative Regulation". (2024, July). Retrieved from https://online.zakon.kz/Document/?doc_id=33690397#sub_id=3200.

[32] Law of the Republic of Kazakhstan No. 94-V "On Personal Data and their Protection". (2013, May). Retrieved from https://adilet.zan.kz/rus/docs/Z1300000094/z13094.htm.

[33] Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, 22(1). doi: 10.1080/1097198X.2019.1569186.

[34] Maksutov, B.M. (2019). The legal mechanism for the protection of personal data in Kazakhstan on the basis of the General Data Protection Regulation (GDPR). In *XI international correspondence scientific specialized conference "International scientific review of the problems of law, sociology and political science"* (pp. 23-35). Boston: Problems of Science.

[35] McGraw, D., & Mandl, K.D. (2021). Privacy protections to encourage use of health-relevant digital data in a learning health system. *NPJ Digital Medicine*, 4, article number 2. doi: 10.1038/s41746-020-00362-8

[36] Mentukh, N., & Shevchuk, O. (2023). Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy and Security*, 1(1), 4-17.

[37] National public data breach: What you need to know. (2024). Retrieved from https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535#:~:text=In%20early%202024,%20National%20Public%20Data,%20an%20online%20background%20check.

[38] Nurgalieva, E.N., & Syrlybaeva, F.M. (2020). Information legal relations in Kazakhstan labour law. *Science*, 64(1), 25-29.

[39] Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan No. 395 "On Approval of the Rules for the Collection and Processing of Personal Data". (2023, April). Retrieved from https://adilet.zan.kz/rus/docs/V2000021498.

[40] Personal data protection in Kazakhstan 2022: Statutory changes and the cases of liability for violations. (2022). Retrieved from https://www2.deloitte.com/kz/en/pages/legal/articles/Personal data protection in Kazakhstan.html.

[41] Podoprigora, R., Apakhayev, N., Zhatkanbayeva, A., Baimakhanova, D., Kim, E.P., & Sartayeva, K.R. (2019). Religious freedom and human rights in Kazakhstan. *Statute Law Review*, 40(2), 113-127. doi: 10.1093/slr/hmx024.

[42] Protection of personal information. (2023). Retrieved from https://www.gov.kz/memleket/entities/mdai/activities/9552?lang=ru&parentId=6.

[43] Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., & Urbach, N. (2019). Building a blockchain application that complies with the EU general data protection regulation. *MIS Quarterly Executive*, 18(4), 7.

[44] Semeniuk, S., & Horbach-Kudria, I. (2024). Administrative legal principles of human rights-based approach by the police. *Law Journal of the National Academy of Internal Affairs*, 14(3), 87-97. doi: 10.56215/naia-chasopis/3.2024.87.

[45] Shahrullah, R.S., Park, J., & Irwansyah, I. (2024). Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment. *Hasanuddin Law Review*, 10(1), 1-20. doi: 10.20956/halrev.v10i1.5016.

[46] Sherif, A. (2024). *Work from home: Remote & hybrid work – statistics & facts*. Retrieved from https://www.statista.com/topics/6565/work-from-home-and-remote-work/#topicOverview.

[47] Sicurella, S. (2024). *AT&T and Ticketmaster breaches show hackers can attack from many angles*. Retrieved from https://www.adn.com/nation-world/2024/07/26/att-and-ticketmaster-breaches-show-hackers-can-attack-from-many-angles/#:~:text=When%20cybercriminals%20stole%20five%20months%20of%20customers%E2%80%99%20call%20logs%20from.

[48] Special Eurobarometer 487a: Summary. (2019). Retrieved from https://cnpd.public.lu/dam-assets/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf#:~:text=This%20Special%20Eurobarometer%20survey%20was%20commission%20ed%20by%20European%20Commission.

[49] Syrlybaeva, F.M. (2022). Some issues of protection of employee information rights. *Bulletin of L.N. Gumilyov Eurasian National University. Law Series*, 140(3), 72-80.

[50] Truong, N., Sun, K., Wang, S., Guitton, F., & Guo, Y. (2021). Privacy preservation in federated learning: An insightful survey from the GDPR perspective. *Computers & Security,* 110, article number 102402. doi: 10.1016/j.cose.2021.102402.

[51] Yakymenko, B. (2023). Formation of the institute of personal data protection and experience of its implementation in the countries of the EU. *Scientific Journal of the National Academy of Internal Affairs*, 28(4), 68-79. doi: 10.56215/naia-herald/4.2023.68.

[52] Yerbolatov, E., Kubenov, G., Zhetpisov, S., Alibaeva, G., & Boretskiy, A. (2020). Personal data in the Republic of Kazakhstan: Problems of ensuring confidentiality in the context of digitalization. *Bulletin of the Innovative University of Eurasia*, 79(3), 49-58.

[53] Zaeem, R.N., & Barber, K.S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems*, 12(1), article number 2. doi: 10.1145/3389685.

Захист інформації про персональні дані працівників у Республіці Казахстан

Фатіма Сирлибаєва

Аспірант
Євразійський національний університет ім. Л.Н. Гумільова
010008, вул. Сатпаєва, 2, м. Астана, Республіка Казахстан
https://orcid.org/0009-0009-2349-0894

Ксенія Касимова

Аспірант
Євразійський національний університет ім. Л.Н. Гумільова
010008, вул. Сатпаєва, 2, м. Астана, Республіка Казахстан
https://orcid.org/0000-0001-7759-209X

Ельміра Омарова

Кандидат наук, доцент
Євразійський національний університет ім. Л.Н. Гумільова
010008, вул. Сатпаєва, 2, м. Астана, Республіка Казахстан
https://orcid.org/0000-0002-2927-7164

Бакит Жусипова

Кандидат наук, доцент
Євразійський національний університет ім. Л.Н. Гумільова
010008, вул. Сатпаєва, 2, м. Астана, Республіка Казахстан
https://orcid.org/0000-0002-2710-2950

Енлік Нургалієва

Доктор наук, професор
Євразійський національний університет ім. Л.Н. Гумільова
010008, вул. Сатпаєва, 2, м. Астана, Республіка Казахстан
https://orcid.org/0009-0002-0568-0765

Анотація. Актуальність даного дослідження обумовлена збільшенням кількості випадків витоку персональних даних громадян, що свідчить про низький рівень захисту їх основних прав. Метою дослідження був аналіз чинного законодавства в контексті забезпечення захисту інформації про персональні дані працівника в Республіці Казахстан. Для цього було використано кілька методів, таких як логічний, формально-юридичний порівняльний аналіз, догматичний метод. Були досліджені норми, які встановлені Конституцією Республіки Казахстан, Трудовим кодексом Республіки Казахстан, Законом Республіки Казахстан " Про затвердження Правил збору та обробки персональних даних". Це дало можливість провести порівняльно-правовий аналіз чинних законодавчих норм Казахстану та європейських нормативно-правових актів. Зазначено, що в правовій доктрині Казахстану не закріплені основоположні принципи, які дозволяють врегулювати питання збору, обробки та зберігання персональних даних громадян. Крім того, на державному рівні не встановлено обов'язок роботодавця та чіткий механізм збереження конфіденційності персональних даних працівників. У зв'язку з цим запропоновано рекомендації щодо вдосконалення чинного законодавства. Практичне значення одержаних результатів полягає в можливості використання запропонованих рекомендацій для підвищення ефективності механізму захисту інформації про персональні дані працівника в Казахстані, зменшення кількості випадків витоку інформації, приведення правових норм у відповідність до міжнародних стандартів

Ключові слова: приватність; права і свободи людини; проліферація; загроза; діджиталізація; безпека