Corporate information about individuals in Uzbekistan (legal protection issues)

Jakhongir Yuldashev

Professor of the Department of Civil Law, Tashkent State University of Law

ABSTRACT

This article presents a scientific and theoretical analysis of the legal protection of personal data of founders, shareholders, investors, creditors , affiliates of joint-stock companies and other persons interested in joint-stock companies operating in Uzbekistan. Based on the results of the study, he put forward proposals for the protection of personal data for joint-stock companies within the framework of the national legislation of Uzbekistan.

Keywords: Joint stock company, company, personal information, founders, shareholders, investors, creditors, affiliates, cybercrime, shareholder legal relations.

The company's information policy also provides for the provision, upon request, of information about the founders, shareholders, investors, creditors, affiliates of the joint-stock company, etc. However, the information provided should not cause inconvenience or negative consequences to the owner of the information in the future as personal information. When generating personal information, it is also important for what purpose it is collected and processed. After all, the legality, truthfulness, reliability and purposefulness of actions taken to collect, systematize, store, change, fill out, use, provide, distribute, transfer, assign and destroy personal data are always relevant.

Information that directly identifies an individual is considered personal information. Today it is no secret that not only competent government agencies, but also companies are involved in the collection and processing of personal data and the formation of existing databases. For example, there is no doubt that corporations collect and process information about their employees or contractors. Because it is important for his interests and business organization. Any citizen can collect certain information about other persons for his own interests.

Personal information is information that individualizes a given person or serves to identify him separately from other individuals. Personal information plays a crucial role in many aspects of our lives. Today, virtual online activities have become much more active, online shopping, interaction and exchange of information on social networks, integration of all interdepartmental information, and the growth of digital information exchange have increased the relevance of this issue and its significance as a subject. protection _ Personal information is important information that should be protected and respected. The collection, processing and use of such data must be transparent and user-friendly. The importance of preventing abuse in the collection, storage, processing and use of personal data is increasing, as well as the importance of maintaining the confidentiality of legally protected secrets (professional, corporate).

This problem becomes clearer when a joint stock company provides, upon request,

information about its shareholders, investors, affiliates, and creditors.

For example, based on the content of Article 86 of the Law "On Joint-Stock Companies and Protection of Shareholders' Rights", an affiliated person is affiliated with a joint-stock company, information about the proposed transaction, including the persons involved in the transaction, information about the subject of the transaction, important details of the relevant agreements must be communicated to the joint stock company by sending a written notice detailing the terms. Information about transactions concluded with affiliated persons, including written statements from affiliated persons and a full description of the decisions made on transactions, information about the persons who made the decisions, as well as information about conflicts of interest when concluding transactions with affiliated persons are part of the annual report of the joint-stock company.[1].

When providing information, it is necessary to pay attention to the identity of affiliated persons of the joint-stock company.

A joint stock company is obliged to notify the joint stock company in writing of its affiliation with a detailed indication of the information specified in these Rules, no later than three working days after establishing the basis for the affiliation [2].

The message about individuals who are affiliates of the joint-stock company must indicate the following information about the affiliates:

- last name, first name, patronymic, place of residence, as well as email address, if available, personal identification code of the individual and a copy of an identity document;

- the basis and date of recognition of them as affiliates of this joint stock company;

- the number, type and percentage of voting shares of the joint-stock company owned by them;

The concept of personal data is defined differently in different literatures. According to Article 3 of the Law of the Republic of Uzbekistan "On Personal Data", personal information is information recorded in electronic form, on paper and (or) on another material body, relating to a specific individual or allowing him to be identified.[3].

Some authors try to explain the concept of personal data within the framework of the concept provided for by current legislation [4. -118 s].

According to Kh. Paluniyazov, "personal information" is information characterizing a specific individual, his physical and social status, which is available openly or confidentially in civil transactions and is important for the implementation and protection of civil rights [5].

According to I. Nasriev, personal information is any identified or identifiable information relating to an individual" [6.-346 p.].

In general, personal data or information is information relating to relevant persons, regardless of the source of their receipt, the form of presentation, different from data about other persons and protected under separate legal documents. Such information is protected by authorized government bodies or the person himself, and measures are taken to prevent threats to the personal safety of the owners of this information (if necessary, the security of society and the state) and eliminate their consequences.

Obtaining personal data is necessary only in accordance with the law and, above all, without prejudice to human rights and freedoms and moral values. Typically, to ensure freedom of information in a country, the state protects the right of every person to seek, receive, verify, disseminate, use and store information. It is not permitted to restrict the right to receive information on the basis of gender, race, nationality, language, religion, social origin, beliefs, personal and social status. However, this provision does not apply to especially protected personal information. Thus, current legislation protects personal data and ensures their legal guarantee through the competent authorities.

No consensus on what information should be included in personal data, on what basis and conditions they should be classified. First name, last name and patronymic of the person, year of birth, month, day, place of birth,

address, nationality, marital status, social status, property status, education, profession, income, telephone number, email address, political and religious views. Personal information may include personal information, health information, criminal records, an individual's personal identification number, savings account number, and taxpayer identification number.

In order to include this data in the proposal on personal data, it is necessary to pay special attention to some cases, that is, among them there are data that can be considered personal data not individually, but several of them together. may become subject to protection. For example, email by itself is not personal information. Because it is impossible to know which person owns a particular email address. Also, a person's last name, first name and patronymic are not always protected as personal information. For example, the name itself is not considered absolute information about a particular person. When processing personal data, the individual (legal entity) to whom this data relates, and the government body, individual and (or) legal entity (operator) involved in the processing of personal data.

It should be understood that the importance of personal data protection is not only the above, but is also important for a person's life and activity, and is also a special factor in his protection. Personal data is a collection of confidential information about each person. Therefore, it is necessary to always understand the importance of this information for its owner. Typically, since personal data is collected and processed by authorized government agencies and some companies, it is their responsibility to protect it. If personal information is disclosed to third parties, it may lead to fraud, defamation and other serious problems. The need to protect personal data is determined by a number of factors. Including:

Dangers and threats. The collection and processing of personal data is fraught with risks and threats. Cybercriminals can exploit security vulnerabilities to gain access to personal data, access the resources on which it is stored, or access the memory of computers on which it is stored, and use it for criminal purposes. Classifying cybercrime, A. Anorboev scientifically analyzes a number of its types and reveals the meaning of social, political and cybercrimes against a person's personality, life and morality [7]. Some authors focus on the distinction between jihad, crimes in the field of information technology and cybercrimes [8]. Data leaks, viruses, and other cyber attacks have become ubiquitous problems on the Internet.

Encryption of personal data. Personal data encryption is a data security method that converts data into an encrypted form that is accessible only to authorized users using a key. This is considered an important mechanism for protecting data during transmission and storage.

Identification of personal data . It is important to register and identify personal data in a computer system. This can be a number or a string of characters indicating the subjects of relationships related to the protection of personal data. This information is called a subject identifier. If a user has an ID registered on the network, he is a legal (legitimate) user, otherwise he is an illegal (illegal) user. Before using computer resources, the user must go through a computer system identification and authentication process.

The protection of personal data is the responsibility of every person who collects and processes this data. Data security is a key aspect of our digital world. This factor helps reduce the risks associated with the illegal receipt, processing and disclosure of personal data, as well as ensuring data confidentiality. Effective protection of personal data is the key to user trust and confidence in the use of modern technologies and services.

According to I. Zakirov, the protection of rights is carried out within the framework established by law, that is, using a certain form, method and means of protection. There are two forms of protection of rights – jurisdictional (through the court) and non-jurisdictional (without the court) [9]. In fact, different tools and methods can be used to protect personal data. In accordance with the above, it can also be divided into jurisdictional and non-jurisdictional remedies.

The jurisdictional form of personal data protection is manifested in the activities of competent government bodies to protect violated or conflicting rights. Its essence is that a person whose rights in relation to personal data have been violated (data owner, custodian, possessor, operator) applies to the authorized government body to restore his rights. Rules related to administrative procedures apply here.

Basically, violated rights are protected in the manner and under the conditions provided for by procedural legislation and regulations.

The form of jurisdictional protection of personal data, in turn, has general (judicial) and special (administrative procedures) procedures for the protection of violated rights.

The non-legal form of personal data protection means that the person whose right is violated acts independently and at his own request, without contacting the state or other authorized body. However, protection must be subject to certain conditions. Measures taken by the owner and (or) operator, as well as third parties to protect personal data, consist of legal, organizational and technical measures. Legal, organizational and technical measures are legal, organizational and technical measures to implement the subject's right to protection from interference in his personal life, maintaining the integrity and completeness of personal data, maintaining data confidentiality and preventing illegal data processing.

According to Article 33 of the Law on Personal Data, persons guilty of violating the legislation on personal data are liable in accordance with the established procedure.

If citizens, in the exercise of their rights and freedoms, cause harm to the legitimate interests, rights and freedoms of the state and society or encroach on social relations protected by law, including in violation of general and private legal norms governing relations related to personal data, as well as ethical rules, in connection with this responsibility arises. Responsibility is the application by the state of coercive measures to the offender on the basis of sanctions provided for by current legislation, in which the guilty persons are deprived of certain rights (personal, property, organizational, etc.).

A person who has received, processed or distributed personal information without a legal basis, or uses it, is subject to liability provided for by law for illegal actions (inaction) and payment of the full amount of damage caused. From the moment when a bona fide owner of personal information learns that such information is being used illegally, if he continues to use the information, he is liable to the owner of the information and is obliged to compensate for the damage caused to him. For this reason, the legal owner of the information must warn the bona fide owner about the illegal use of the information. An unscrupulous owner of personal information is liable from the moment the information is received, distributed or used. A person lawfully in possession of such information has the right to request that such use cease as soon as it becomes aware that others are using the information unlawfully.

Improving legislation on information policy in Uzbekistan can serve to increase transparency, responsibility and corporate governance in joint-stock companies. Improve such legislation, tighten requirements for information disclosure, protect the confidentiality of information, ensure transparency of corporate governance, monitor the inevitability of punishment for violations, analyze international standards and best practices, information policy. for certain specialized, state and monopoly joint-stock companies, it is necessary to improve legislative documents in terms of defining special requirements.

References

1. Law of the Republic of Uzbekistan "On joint-stock companies and protection of shareholders' rights"// https://lex.uz/docs/4617583
2. "Правила предоставления и публикации информации на рынке ценных бумаг" утвержденные приказом генерального директора Центра по координации и развитию рынка ценных бумаг при Госкомконкуренции Республики

Узбекистан от 22 сентября 2014 года № 2014-28 (рег. № 2383-2 от 09.10.2014 г.)//https://lex.uz/acts/2038449#2480226
3. Law of the Republic of Uzbekistan “On personal data»// https://lex.uz/docs/4831939
4. Назаров Д.М., Саматов К.М. Основы обеспечения безопасности персональных данных в организации. -Екатеринбург. Изд Урал. Гос. экон. ун-та, 2019 -118 с.
5. Палуаниязов Х.А “Шахсга тааллуқли маълумотларни фуқаролик-ҳуқуқий муҳофаза қилиш. Ю.ф.н.дисс. Автореферат. -Т. 2009.
6. Насриев И.И. Шахсий номулкий ҳуқуқларни амалга ошириш ва муҳофаза қилишнинг фуқаролик-ҳуқуқий муаммолари.: Дисс. ... док. юрид. наук. Тошкент: ТГЮИ. 2006. - С. 346.
7. Анорбоев А. Кибержиноятларнинг жиноий-ҳуқуқий жиҳатлари. Ю.ф.ф.д. илмий даражасини олиш учун ёзилган диссертация. –Тошкент, 2021. 294/
8. Салаев Н. Рузиев Р. Кибержиноятчиликка ыарши курашишга оид миллий ва халқаро стандартлар. –Т.: ТДЮУ. 2018. -139 б.
9. Зокиров И. Фуқаролик ҳуқуқи. -Т.: ТДЮИ 2009.
10. Imomniyozov, D. (2023). KORPORATSIYA IJRO ORGANI RAHBARI BILAN TUZILADIGAN SHARTNOMANING HUQUQIY TABIATI. Oriental renaissance: Innovative, educational, natural and social sciences, 3(2), 618-624.
11. Asadov, S. (2023). CONSULTING SERVICES: RIGHTS AND OBLIGATIONS OF THE PARTIES. International Bulletin of Applied Science and Technology, 3(1), 142-145.
12. Koryogdiev, B. U. U., & Nechaeva, E. V. (2022). DEFENSE MECHANISMS AGAINST HOSTILE TAKEOVERS (COMPARATIVE ANALYZE). Oriental renaissance: Innovative, educational, natural and social sciences, 2(2), 124-135.