



Funded by the
European Union

INIDI

ERKINDIK
QANATY
общественный фонд

INSTITUTE FOR
WAR & PEACE REPORTING



ИНСТИТУТ РЕПОРТАЖЕЙ ВОЙНЫ И МИРА

PERSONAL DATA PROTECTION IN NGOs: CHALLENGES AND SOLUTIONS

POLICY BRIEF

This publication was funded by the European Union. Its contents are the sole responsibility of IWPR and do not necessarily reflect the views of the European Union.

2025

Contents

5	INTRODUCTION
7	INTERNATIONAL STANDARDS FOR PERSONAL DATA PROTECTION
11	LEGAL REGULATION OF PERSONAL DATA PROTECTION IN KAZAKHSTAN
24	ANALYSIS OF THE RESULTS OF A SURVEY ON PERSONAL DATA PROTECTION IN PUBLIC ORGANIZATIONS OF KAZAKHSTAN, CONDUCTED BY THE PUBLIC FOUNDATION «ERKINDIK QANATY» IN FEBRUARY–MARCH 2025
34	ANALYSIS OF THE RESULTS OF FOCUS GROUPS ON THE PROTECTION OF PERSONAL DATA IN PUBLIC ORGANIZATIONS OF KAZAKHSTAN, CONDUCTED BY THE PF «ERKINDIK QANATY» IN FEBRUARY–MARCH 2025
40	CHALLENGES AND RISKS RELATED TO PERSONAL DATA PROTECTION IN PUBLIC ORGANIZATIONS
42	RECOMMENDATIONS
45	CONCLUSION
47	REFERENCES



ABOUT THE AUTHOR

Kuralay Karakulova, Lawyer, Master of Laws.
Certified Global Trainer on Human Rights and Women's Rights (WLP USA).
Expert on Gender Equality.
Legal Expert for the UNDP in Kazakhstan.
Member of the Eurasian Chamber of Lawyers, Almaty.

ABOUT THE FOUNDATION

PF Wings of Liberty was established on March 6, 2015. The Foundation is an open type human rights organization that has accumulated experience and values gained in the process of forming an active citizenship of the organizers and volunteers of the Foundation. The main directions of the Foundation's work are public protection and promotion of rights and freedoms, educational programs, conducting research, including through monitoring, as well as participation in law-making.



ABOUT IWPR

IWPR empowers local voices to drive change in countries in conflict, crisis and transition.

Where hate speech and propaganda proliferate, and journalists and civic activists are under attack, IWPR promotes reliable information and public debate that makes a difference. With powerful new forms of disinformation driving social division, increasing digital security risks and escalating attacks on journalists, IWPR's mission to empower local voices is more important than ever. IWPR's core work is to strengthen the flow of credible, unbiased information, enabling journalists and civil society to inform, educate and mobilise communities. IWPR empowers societies to find their own solutions, by strengthening local capacity to report on and advocate for accountability, freedom of expression and human rights.

ABOUT THE EUROPEAN UNION

The European Union is an economic and political union of 27 European countries. It is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. It acts globally to promote sustainable development of societies, environment and economies, so that everyone can benefit.



POLICY BRIEF

This policy brief has been prepared as part of the «Civil Society for Kazakhstan (CS4K)» Project, implemented by the Institute for War and Peace Reporting (IWPR) in partnership with the Institute for National and International Development Initiatives (INIDI) with the financial support from the European Union.

The project aims to promote fundamental freedoms and rights in Kazakhstan through the efforts of civil society.

INTRODUCTION

Nowadays, the modern world is rightfully called the digital world. At the same time, the introduction of digital technologies occurs with the use of information.

The volume of information transmitted via the Internet is growing rapidly. This includes registration in online services, the use of social networks and mobile applications, and all this is accompanied by the transfer of a person's personal information.

But not many people think about the fact that by providing information about themselves, they consciously or unconsciously provide other people with their personal data.

After all, information about a person is sensitive personal data, which makes it vulnerable to fraud, threats, theft and negative impact on the owner of the information.

Meanwhile, it should be noted that personal information, personal data are directly related to ensuring the fundamental rights and freedoms of a person, in particular **the right to privacy, personal privacy and dignity of the individual.**

This right was first regulated in the **Universal Declaration of Human Rights** in Article 12 – «No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.»¹

Later, this right was enshrined in the **International Covenant on Civil and Political Rights** in Article 17 – «No one shall be subjected to arbitrary or unlawful

¹ Universal Declaration of Human Rights, Adopted by resolution 217A (III) of the UN General Assembly on 10 December 1948.



interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.»²

Personal data is part of a person's private life. Their illegal collection and dissemination may lead to violation of **human rights**.

Therefore, the protection of personal data is currently a pressing issue not only at the international but also at the national level. Kazakhstan is no exception and is developing the main directions of state policy in the field of personal data and their protection at the legislative level.

The key aspects of personal data protection in Kazakhstan are:

- 1) establishment of clear legal guarantees for the protection of personal data;
- 2) ensuring the protection of the rights of personal data subjects;
- 3) implementation of information and technical solutions for data protection, as well as the development of cybersecurity.
- 4) taking measures to hold accountable persons who have violated the legislation on personal data and their protection.

States, organizations and societies as a whole are responsible for ensuring that digital technologies and mechanisms for collecting and processing personal data do not violate the fundamental freedoms of citizens.

² International Covenant on Civil and Political Rights, Adopted by General Assembly resolution 2200 A (XXI) of 16 December 1966.



INTERNATIONAL STANDARDS FOR PERSONAL DATA PROTECTION

International regulation of personal data protection is an important aspect, especially in the context of globalization and growth of data volumes.

Different countries set their own rules, regulations, but **international documents and principles** have been formed that combine these efforts and ultimately provide a unified approach to the protection of privacy.

And such a main international document was **Regulation No. 2016/679 of the European Parliament and of the Council of the European Union of 27 April 2016 «On the protection of individuals with regard to the processing of personal data and on the free movement of such data** (GDPR – General Data Protection Regulation). The Regulation is called the main international standard adopted in the European Union, which entered into force on 25 May 2018.

The purpose of this Regulation is to protect individuals with regard to the processing of personal data and the rules for the free movement of personal data. As well as the protection of the fundamental rights and freedoms of individuals and, in particular, the right to the protection of personal data.

An important point is that the Regulation represents unified rules for the EU, i.e. uniform rules concerning the processing of personal data.

Moreover, the Regulation established universal principles for the processing of personal data:



Article 5. Principles of personal data processing

- a. processed lawfully, fairly, and in the manner intended for the data subject («lawfulness, fairness and transparency»);
- b. collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- c. are adequate, relevant and include only what is necessary for the purposes of the processing («data minimization»);
- d. are accurate and, where necessary, updated; all reasonable steps must be taken to ensure that inaccurate data is deleted or rectified without delay, taking into account the purposes for which they are processed («accuracy»).
- e. stored in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- f. processed in a manner that ensures the security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage through the application of appropriate technical or organizational measures («integrity and confidentiality»).

These principles have extraterritorial regulation, which means that all government agencies, organizations, and companies collecting, processing, and storing personal data of individuals must comply with the principles of the EU General Regulation.

The key feature of this regulation is that it very broadly defines the concept of «personal data».

Article 4 Definitions

«**Personal data**» means any information relating to an identified or identifiable natural person («data subject»); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, surname, identification number, location data, online identifier or to one or more physical, physiological, genetic, mental, economic, cultural or social identity factors specific to that person;

In addition, the Regulation contains a mandatory requirement to obtain consent for the use and processing of data, as well as the right to delete data and the appointment of a personal data protection specialist in organizations.



The next international document is the «Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data» adopted by the members of the Council of Europe on 28 January 1981, one of the first documents on this issue. «The purpose of this Convention is to ensure in the territory of each Party respect for the rights and fundamental freedoms of every individual, whatever his nationality or place of residence, and in particular his right to privacy with regard to automatic processing of personal data relating to him («data protection»).

³ It should also be noted that similar documents on the protection of personal data have been adopted in the countries of the Asia–Pacific region, in Canada, Brazil and in some African countries.

All of these documents support voluntary principles of privacy and focus on the balance between the protection of rights and freedoms and business development.

The United Nations (UN) recognizes the importance of protecting personal data and has developed a number of recommendations and principles aimed at ensuring the confidentiality and security of personal information.

One of the first documents was General Assembly Resolution 68/167 of 18 December 2013. The right to privacy in the digital age. The main message of this resolution to all states is to respect and protect the right to privacy, including in the context of digital communication. And also to take measures to respect the rights of personal information subjects, prevent violations, and bring national legislation in line with international obligations under international human rights law.

³ «Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data» adopted by the members of the Council of Europe on 28 January 1981.



UN Resolutions, Policies Regulating Personal Data Protection Issues

- General Assembly resolution 69/166 of 18 December 2014
The right to privacy in the digital age
- UNHCR Policy on the Protection of Personal Data of Persons of Concern, 2015
- Principles on the Protection of Personal Data and Privacy (adopted by the UN High-Level Committee on Management (HLCM) at its 36th meeting on 11 October 2018).
- Human Rights Council resolution 48/4 of 7 October 2021
- UNHCR General Data and Privacy Policy (GDPP), 2022

In addition, the UN established the Special Rapporteur on the right to privacy in March 2015.

The Special Rapporteur's mandate empowers him to promote and protect the right to privacy by:

- Reviewing government policies and laws on the interception of digital communications and the collection of personal data
- Identifying acts that violate privacy without good cause
- Assisting governments in developing best practices for global surveillance in line with the rule of law
- Articulating the private sector's responsibilities to respect human rights
- Assisting in ensuring that national policies and laws comply with international human rights obligations.

Governments, businesses, and civil society organizations must follow these international standards to be open, safe, and legitimate in the eyes of their partners and citizens.



LEGAL REGULATION OF PERSONAL DATA PROTECTION IN KAZAKHSTAN

According to Article 18 of the Constitution of the Republic of Kazakhstan, «Everyone has the right to privacy, personal and family secrets, and protection of their honor and dignity.»⁴ This constitutional norm indicates that, according to the Constitution, the most protected information in the state, along with information constituting a state secret, is information about a person's private life.

(Comments to Article 10 of the Civil Procedure Code of the Republic of Kazakhstan).

«Private life is a sphere of activity of one individual, which is dear only to him, therefore interference from society, the state without the consent of the person is unacceptable. Personal secret, being a part of private life, implies the presence of information that a person keeps secret. This may include information concerning health, details of intimate life, etc. Family secret implies the presence of information hidden from outsiders by close relatives, i.e. family members. This includes the secret of adoption and other relationships in the family. Considering the great importance of a person's private life, the legislator recognizes it as inviolable and protects it from any illegal interference.»

Since personal data includes information about a person's private life, it is necessary to ensure the right to privacy, the right to personal and family secrets in relation to the processing of personal data and their protection.

Later, the constitutional norm was regulated by adopting a special law. Thus, on May 21, 2013, the **Law of the Republic of Kazakhstan «On Personal Data and Their Protection»** (hereinafter referred to as the Law) was adopted.

According to Article 2 of the Law, the purpose of this Law is to ensure the protection of the rights and freedoms of a person and citizen when collecting and processing his personal data.⁵

An important aspect of the Law is to enshrine the principles of personal data protection. Thus, in accordance with Article 5 of the Law, the Collection, processing and protection of personal data are carried out in accordance with the following principles:

⁴ The Constitution of the Republic of Kazakhstan, adopted at the republican referendum on August 30, 1995.

⁵ The Law of the Republic of Kazakhstan «On personal data and their protection» was adopted on May 21, 2013 No. 94-V.



- 1) compliance with the constitutional rights and freedoms of a person and citizen;
- 2) legality;
- 3) confidentiality of personal data of limited access;
- 4) equality of rights of subjects, owners and operators;
- 5) ensuring the security of the individual, society and the state.

It should be especially noted that the **subject of personal data is only an individual** to whom the personal data relates, i.e. the carrier of personal data.

According to the definition adopted by the Law, **personal data is information related to a specific or determinable subject of personal data, recorded on electronic, paper and (or) other tangible media.**

In this case, personal data is any information that in one way or another relates to the subject of personal data, including both direct and indirect features that allow identifying a person. In practice, personal data includes the last name, first name, patronymic, date of birth, citizenship, education, marital status, residential address and other information about the subject.

At the same time, personal data are divided by availability into publicly available and restricted access.

Publicly available personal data are personal data or information that, in accordance with the laws of the Republic of Kazakhstan, are not subject to confidentiality requirements, access to which is free with the consent of the subject.

Restricted access personal data are personal data, access to which is restricted by the legislation of the Republic of Kazakhstan.

According to paragraph 3 of the Rules for the implementation of measures to protect personal data by the owner and (or) operator, as well as a third party, threats to the security of personal data are understood as a set of conditions and factors that create the possibility of unauthorized, including accidental, access to personal data during their collection and processing, which may result in the destruction, modification, blocking, copying, unauthorized provision to third parties, unauthorized distribution of personal data, as well as other illegal actions.

In accordance with Article 8 of the Law, Consent to the collection and processing of personal data includes:

Item 4, Article 8 of the Law «On Personal Data and Their Protection»

- 1) the name (last name, first name, surname (if indicated in the identity document), business identification number (individual identification number) of the operator;
- 2) last name, first name, surname (if indicated in the identity document) of the subject;
- 3) the term or period during which consent to the collection and processing of personal data is valid;
- 4) information about the operator's ability or lack thereof to transfer personal data to third parties;
- 5) information about the presence or absence of cross-border transfer of personal data in the process of their processing;
- 6) information about the dissemination of personal data in publicly available sources;
- 7) a list of collected data related to the subject;
- 8) other information determined by the owner and (or) operator.

Particular attention should be paid to subparagraph 8 other information determined by the owner and (or) operator. This norm is optional, which in turn creates risks of collecting various information that can be used to manipulate the owner of personal data. Meanwhile, it is worth noting that Article 14 of the Law «On Personal Data and Their Protection» stipulates that the use of personal data must be carried out by the owner, operator and third party only for the previously declared purposes of their collection. That is, the collection of the volume (quantity) of information/ data about the subject must be solely based on the declared purposes, otherwise the collection of information without a purpose will be considered illegal.

One of the main requirements for the collection and processing of personal data is to ensure their protection.

According to paragraph 11 of Article 1 of the Law, **the protection of personal data is a set of measures, including legal, organizational and technical**, carried out for the purposes established by this Law.

The adopted norm indicates that when working with personal data, it is necessary to take appropriate measures to protect personal data.



For these purposes, the Law adopts the legal basis for activities related to the collection, processing and protection of personal data, which includes the following legal and organizational measures:

- ✓ Protection of personal data
- ✓ Collection of personal data
- ✓ Accumulation of personal data
- ✓ Storage of personal data
- ✓ Processing of personal data
- ✓ Changing personal data
- ✓ Supplementing personal data
- ✓ Using personal data
- ✓ Distributing personal data
- ✓ Depersonalization of personal data
- ✓ Blocking of personal data
- ✓ Destruction of personal data

It should be especially noted that the Law establishes the rights and obligations of entities that are responsible to one degree or another for working with the protection of personal data.

Such entities are:

1. **an individual** to whom the personal data relates;
2. **the owner of the database** represented by a government agency, an individual and (or) a legal entity exercising the right of ownership, use and disposal of the database containing personal data;
3. **the database operator** represented by a government agency, an individual and (or) a legal entity that collects, processes and protects personal data.
4. **third party** – not being the subject, owner and (or) operator, but connected with them by circumstances or legal relations on the collection, processing and protection of personal data.

In the context under consideration, public organizations are database operators that collect, process and protect personal data.

The Law sets out the competencies of government agencies that implement government regulation in the field of personal data, while an authorized body is defined.



The state authorized body in this case is the **Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan (Information Security Committee)**.

Article 27–1 Competence of the authorized body

- 1) formulates and implements state policy in the sphere of personal data and their protection;
 - 1–1) exercises state control over compliance with the legislation of the Republic of Kazakhstan on personal data and their protection;
- 2) develops the procedure for the implementation of measures to protect personal data by the owner and (or) operator, as well as a third party;
 - 2–1) develops the rules for determining the list of personal data by the owner and (or) operator that is necessary and sufficient to perform the tasks they carry out;
 - 2–2) determines the procedure for determining the list of personal data by the owner and (or) operator that is necessary and sufficient to perform the tasks they carry out;
 - 2–3) determines the procedure for the implementation of measures to protect personal data by the owner and (or) operator, as well as a third party;
- 3) considers appeals from the subject or his legal representative regarding the compliance of the content of personal data and the methods of their processing with the purposes of their processing and makes an appropriate decision;
- 4) takes measures to bring persons who have violated the legislation of the Republic of Kazakhstan on personal data and their protection to liability established by the laws of the Republic of Kazakhstan;
- 5) requires the owner and (or) operator, as well as a third party, to clarify, block or destroy inaccurate or illegally obtained personal data;
- 6) implements measures aimed at improving the protection of the rights of subjects;
 - 6–1) creates an advisory board on personal data and their protection, and determines the procedure for its formation and activities;
 - 6–2) sends information to the operator of the information and communication infrastructure of the «electronic government» on a violation of the security of personal data that entails the risk of violating the rights and legitimate interests of subjects;



- 7) approves the rules for collecting and processing personal data;
- 7-1) approves the rules for conducting an inspection of the security of the processes of storing, processing and disseminating personal data of restricted access contained in electronic information resources, in agreement with the National Security Committee of the Republic of Kazakhstan;
- 7-2) approves the rules for the operation of the state service for controlling access to personal data;
- 7-3) coordinates the integration of non-state information technology facilities with information technology facilities of state bodies and (or) state legal entities, during which personal data is transferred and (or) access to personal data is provided;
- 7-4) approves the rules for integration with the state service for controlling access to personal data;
- 8) exercises other powers provided for by this Law, other laws of the Republic of Kazakhstan, acts of the President of the Republic of Kazakhstan and the Government of the Republic of Kazakhstan.

It is worth paying attention to an important provision in the Law, this is Article 27-2, which provides for state control over compliance with the legislation of the Republic of Kazakhstan on personal data and their protection, carried out in the form of an unscheduled inspection in accordance with the Entrepreneurial Code.

According to this provision, the state authorized body has the right to monitor organizations, including non-profit organizations, for compliance with the Law «On Personal Data and Their Protection».

For reference: statistical data

Since the beginning of 2024, to date, 11 unscheduled inspections have been conducted and 23 administrative cases have been initiated and considered for violation of the requirements of the legislation of the Republic of Kazakhstan in the field of personal data and their protection, as a result of which, under various parts of Articles 79 and 641 of the Code of Administrative Offenses of the Republic of Kazakhstan, 4 individuals and 25 legal entities and officials were brought to justice, fines were imposed for a total of 4,910,360 tenge.

Source: Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan.



At the same time, it is not possible to determine how much the dynamics of administrative liability changes, since the authorized body does not publish such information on its website.

Meanwhile, we can view some dynamics in open sources on the Internet. Thus, according to data from finprom.kz, in January–July of this year, 65 administrative violations of the law on personal data and their protection were registered in Kazakhstan – 75.7 % more than in the same period of 2023. At the same time, 61 cases were considered against only 23 a year earlier. Decisions on administrative liability were issued against 61 people – 2.9 times more than in January–July last year. Fines of 10.1 million tenge were imposed for violations of the law in the sector, 8.1 million tenge were collected. The next open source Liter.kz reports that in 2024, 60 unscheduled inspections and administrative proceedings were conducted in the field of personal data protection for a total of 12 million 153 thousand 455 tenge. This is significantly more than in 2023, when 38 such inspections were registered.

This source also quotes the Chairman of the Committee on Information Security of the MCRIAP RK Ruslan Abdikalikov, who announced the following data: «In the area of information security, 210 unscheduled inspections and administrative cases without on-site visits were conducted during the year for a total of 7 million 817 thousand 810 tenge. In the area of electronic documents and EDS, 10 administrative cases were considered for a total of 304 thousand 519 tenge.»⁶

Thus, it should be noted that the number of administrative cases for violation of the law on personal data has increased. This trend indicates that it is necessary to strengthen work on the security of personal data and carry out measures to improve the level of digital literacy not only of citizens, but also of representatives of legal entities.

It must be said that today the sphere of personal data is under strict control of the state. Thus, according to the Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated April 29, 2022 No. 144 / NK, the Rules for the functioning of the state service for controlling access to personal data were approved.

The State Service for Controlling Access to Personal Data (hereinafter referred to as the KDP Service) is designed to provide access to personal data after receiving

⁶ <https://liter.kz/v-kazakhstane-proveli-proverki-na-12-mln-tenge-v-sfere-zashchity-personalnykh-dannykh-1742455826/>



the relevant consent from the citizen, by sending an SMS message from 1414 with a request for access to personal data or in another way from the subject of personal data.

According to the Law, the KDP Service is mandatory in the case of interaction with information technology objects of state bodies containing personal data.

Thus, to date, 81 information systems are integrated with the KDP Service: 35 of them are state information systems, 9 information systems of the quasi-public sector, 37 private information systems.

The KDP Service allows citizens to control the use of their personal data contained in state databases by granting permission or denying access to them.

Regulatory legal acts for regulating the functioning and integration with the KDP Service:

Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated April 29, 2022 No. 144/HK «On approval of the Rules for the functioning of the state service for controlling access to personal data» (Registered in the Ministry of Justice of the Republic of Kazakhstan on May 7, 2022 No. 27963);

Order of the Acting Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated July 8, 2022 No. 236/HK «On approval of the Rules for integration with the state service for controlling access to personal data» (Registered in the Ministry of Justice of the Republic of Kazakhstan on July 13, 2022 No. 28786).

The state continues to work on paying close attention to compliance with the law on the protection of personal data.

This is confirmed by the fact that on March 28, 2023, the Concept of digital transformation, development of the information technology industry and cybersecurity for 2023–2029 was approved. (Approved by the Decree of the Government of the Republic of Kazakhstan dated March 28, 2023 No. 269.)

Within the framework of the Concept, target indicator 10 «The share of state information systems connected to the personal data access control service» provides for 2 activities, for the first activity, the implementation deadline is scheduled for December 2025, for the second activity, implementation is provided on an annual basis.



The first measure envisages accession to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the Convention was adopted in 1981 by the Council of Europe, known as «Convention 108»)

This is the first international treaty dedicated to the right of individuals to the protection of their personal data.

This Convention will give the right to investigate violations of the rights of our citizens in the field of personal data protection committed by operators of countries that have acceded to the Convention.

The second event provides for the Annual monitoring of state information systems subject to integration with the personal data access control system.

In this regard, it should be noted that the state is taking appropriate measures to comprehensively analyze all necessary procedures and legislative work on the implementation of the norms of the Convention and the GDPR. According to Article 29 of the Law, liability is established for violation of the legislation on personal data and their protection.

The Committee on Information Security of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan is vested with the authority to bring persons to administrative responsibility for violating the requirements of the legislation on personal data and their protection, electronic documents and electronic digital signatures.

Thus, the Committee on Information Security considers cases of administrative offenses in the specified areas, provided for in Articles 79, 640 and 641 of the Code of Administrative Offenses of the Republic of Kazakhstan. The statistics on bringing administrative responsibility are given above.



Code of Administrative Offenses of the Republic of Kazakhstan dated July 5, 2014

Article 79. Violation of the legislation of the Republic of Kazakhstan on personal data and their protection

1. Illegal collection and (or) processing of personal data, if these acts do not contain elements of a criminal offense, – shall entail a fine for individuals in the amount of thirty, for officials, private notaries, private bailiffs, lawyers, legal consultants, small business entities or non-profit organizations – in the amount of sixty monthly calculation indices.
2. The same acts committed by the owner, operator or third party using their official position, if these actions do not entail criminal liability established by law – shall entail a fine for individuals in the amount of one hundred, for officials, small business entities or non-profit organizations – in the amount of two hundred monthly calculation indices.
3. Failure by the owner, operator or third party to comply with measures to protect personal data, if this act does not contain elements of a criminally punishable act, shall entail a fine for individuals in the amount of one hundred and fifty, and for officials, small business entities or non-profit organizations – in the amount of three hundred monthly calculation indices.
4. The act provided for in part three of this article, which resulted in the loss, illegal collection and (or) processing of personal data, if these acts do not entail criminal liability established by law, – shall entail a fine for individuals in the amount of two hundred, for officials, small business entities or non-profit organizations – in the amount of seven hundred and fifty monthly calculation indices.

Article 30 of the Law provides for the protection of the rights of personal data subjects. The actions (inaction) of the subject, owner and (or) operator, as well as a third party in the collection, processing and protection of personal data may be appealed in the manner established by the laws of the Republic of Kazakhstan.

With the adoption of the Law «**On Personal Data and Their Protection**», the Republic of Kazakhstan began to create a special legislative framework for the protection of personal data.

Below is a list of some codes, laws, regulatory legal acts governing the activities to protect personal data.



№	Name of regulatory legal acts	
1.	Labor Code.	from November 23, 2015 No. 414-V.
2.	Social Code.	from April 20, 2023 No. 224-VII ZRK.
3.	Code «On Public Health and the Healthcare System».	from July 7, 2020 No. 360-VI.
4.	Entrepreneurial Code.	from October 29, 2015 No. 375-V.
5.	Constitutional Law «On the Prosecutor's Office».	from November 5, 2022 No. 155-VII.
6.	Law «On Online Platforms and Online Advertising».	from July 10, 2023 No. 18-VIII 3RK.
7.	Law «On State Statistics».	from March 19, 2010 No. 257-IV.
8.	Law «On Informatization».	from November 24, 2015 No. 418-V.
9.	Law «On state regulation, control and supervision of the financial market and financial organizations».	from July 4, 2003 No. 474-II.
10.	Rules for the collection and processing of personal data.	Order of the Minister of Digital Development, Innovation and Aerospace Industry dated October 21, 2020 No. 395/HK.
11.	Rules for the implementation by the owner and/or operator, as well as a third party, of measures to protect personal data.	Order of the Minister of Digital Development, Innovation and Aerospace Industry dated June 12, 2023 No. 179/HK.



12.	Rules for determining by the owner and/or operator the list of personal data necessary and sufficient to perform the tasks they carry out.	Order of the Minister of Digital Development, Innovation and Aerospace Industry dated June 21, 2023 No. 199/HK.
13.	Rules for the implementation of a survey to ensure the security of processes for storing, processing and distributing personal data of restricted access contained in electronic information resources.	Order of the Minister of Digital Development, Innovation and Aerospace Industry dated April 30, 2021 No. 156/HK.
14.	List of personal data necessary and sufficient for the performance of tasks carried out by the Agency for Strategic Planning and Reform, Bureau of National Statistics.	Order of the Chairman of the Agency for Strategic Planning and Reforms dated June 24, 2022 No. 3.
15.	Rules for notifying personal data subjects about a breach of personal data security.	Order of the Acting Minister of Digital Development, Innovation and Aerospace Industry dated August 9, 2024 No. 481/HK.
16.	On some issues of the advisory council on personal data and their protection.	Order of the Minister of Digital Development, Innovation and Aerospace Industry dated April 12, 2022 No. 118/HK.
17.	Rules for the operation of the state service for controlling access to personal data.	Order of the Minister of Digital Development, Innovation and Aerospace Industry dated April 29, 2022 No. 144/HK.



18.	Checklist for compliance with legislation on personal data and its protection in relation to owners and/or operators, as well as third parties.	Joint order of the Minister of Digital Development, Innovation and Aerospace Industry dated March 19, 2024 No. 149/HK and the order of the Deputy Prime Minister – Minister of National Economy dated March 19, 2024 No. 12.
19.	Rules for integration with the state service for controlling access to personal data.	Order of the Acting Minister of Digital Development, Innovation and Aerospace Industry dated July 8, 2022 No. 236/HK.
20.	Storage and transfer of personal data with limited access is carried out using cryptographic information protection tools with parameters not lower than the third security level.	Standard RK STRK1073–2007 «Means of cryptographic protection of information. General technical requirements».

Thus, taking into account global trends and challenges in the field of data security, Kazakhstan strives to create an effective protection system that complies with international principles.



ANALYSIS OF THE RESULTS OF A SURVEY ON PERSONAL DATA PROTECTION IN PUBLIC ORGANIZATIONS OF KAZAKHSTAN, CONDUCTED BY THE PUBLIC FOUNDATION «ERKINDIK QANATY» IN FEBRUARY–MARCH 2025⁷

In the period from February to March 2025, the Public Foundation «Erkindik Qanaty» conducted a survey among non-profit organizations (hereinafter referred to as NPOs) on the issue of personal data protection in public organizations of Kazakhstan.

The purpose of this online survey was to study the practices of personal data protection in non-profit organizations of Kazakhstan.

Two types of methods were used in the study: online questionnaire and focus groups.

Representatives of 117 non-profit organizations from various regions of Kazakhstan took part in the online survey.

It should be noted that as of April 2023, the number of registered NGOs is 23,335. (Source: Information Committee of the Ministry of Information and Culture of the Republic of Kazakhstan.)⁸

To analyze the results of the survey, responses were selected from **111 organizations** that have state registration with the authorized state body.

The questionnaire consists of 33 questions and is divided into sections. For analysis, answers to more relevant questions that reveal the purpose of the study were selected.

⁷ Analysis of the results of a survey on personal data protection in public organizations of Kazakhstan, conducted by the Public Foundation «Erkindik Qanaty» in February–March 2025.

⁸ <https://www.gov.kz/memleket/entities/inf/activities/142?lang=ru>



SURVEY RESULTS

1.1 The first section of the questionnaire reflected basic administrative and organizational information about the organization.

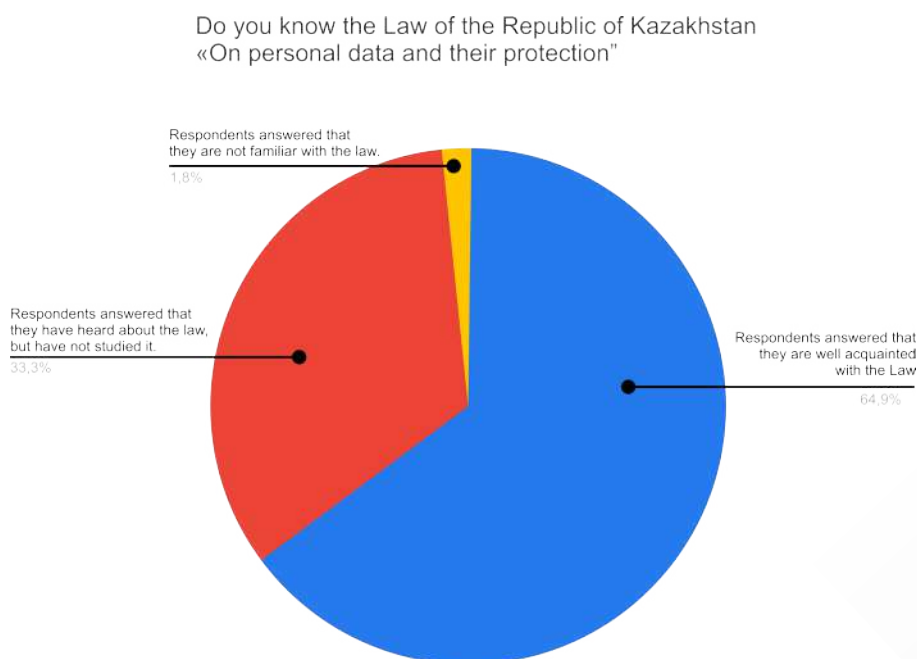
Non-profit organizations from 17 regions of Kazakhstan took part in the survey. The largest number of responses came from the city of Almaty – 27 (23.5 %), the city of Astana – 17 (14.8 %), Kostanay region – 8 (7.0 %), East Kazakhstan region – 8 (7.0 %), Pavlodar region – 7 (6.1 %) and Turkestan region – 7 (6.1 %).

According to the number of staff/volunteers in the organization, it was shown that most organizations have less than 10 employees or volunteers: from 5 to 10 people – 38.9 %, less than 5 people – 36.3 %.

To what extent the organization was active through the implementation of certain projects in 2024, it turned out that more than half of the organizations (55.8 %) implemented from 1 to 5 projects, while 14.2 % did not implement a single project. And only 9.7 % have carried out more than 10 projects.

The survey showed that the largest number of organizations surveyed (35.2 %) work in the field of human rights, followed by the field of education (16.4 %), and in third place is the field of ecology, where they work (11.4 %).

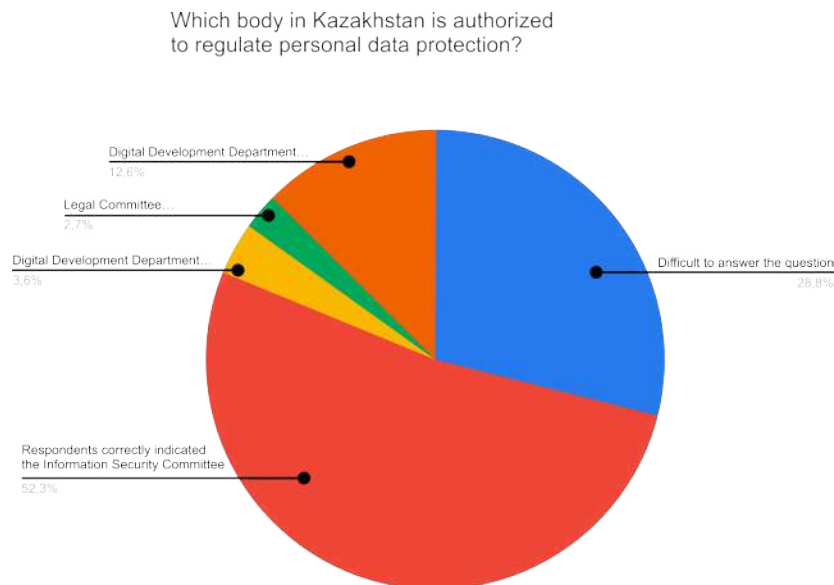
1.2 The second section of the survey was devoted to questions of awareness of personal data protection.





To the survey question Do you know the Law of the Republic of Kazakhstan «On personal data and their protection», 64.9 % of respondents answered that they are well acquainted with the Law «On personal data and their protection». However, 33.3 % of respondents answered that they have heard about the law, but have not studied it.

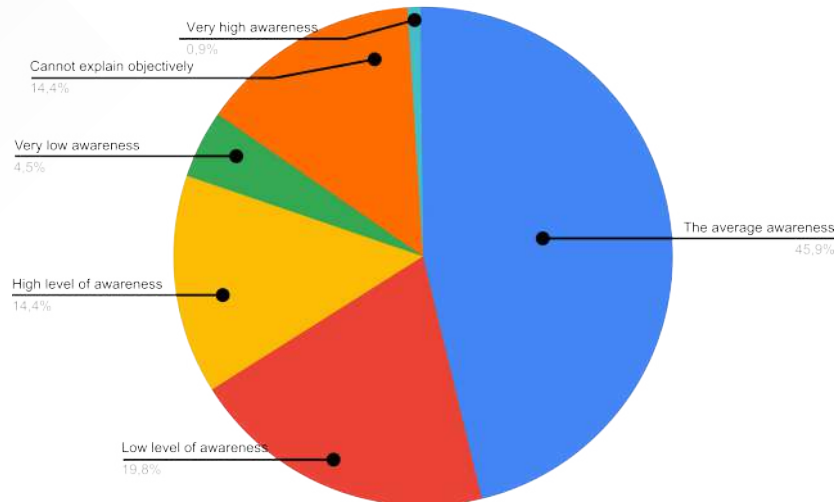
At the same time, 52.3 % of respondents correctly indicated the Information Security Committee under the International Center for Information Security and Anti-Corruption as the authorized body.



However, a third of respondents (28.8 %) found it difficult to answer the question which government agency is responsible for regulating this area. The rest of the respondents chose incorrect answers or did not know the answer at all.

Furthermore, it should be noted that when assessing the level of awareness of personal data protection directly by the organization's team, the average awareness is 45.9 %. Respondents consider their colleagues' knowledge to be average, and only 14.4 % assess the level of awareness as high.

How do you assess your team's level of knowledge about personal data protection?

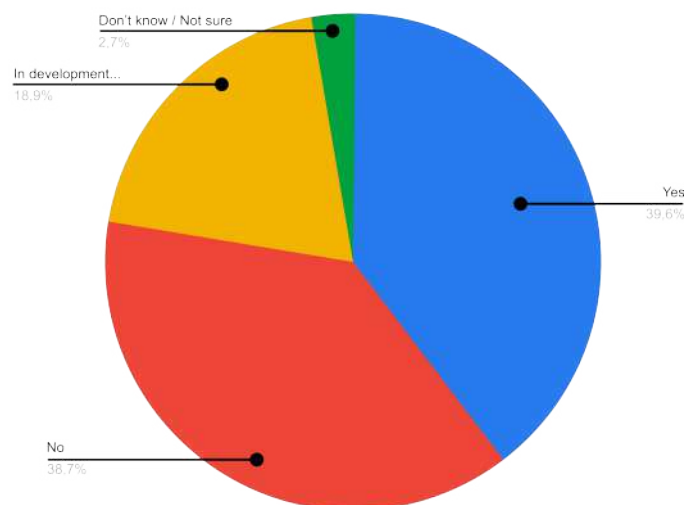


A low level of awareness was noted by 19.8 % of respondents.

3.1. The third section of the survey concerns the current practice of personal data management in the organization.

So, when asked whether the organization has regulations/provisions on the collection, processing, and storage of personal data, only 39.6 % of organizations indicated that they have internal policies and/or regulations on data processing, and 38.7% do not have such documents at all. At the same time, 18.9 % of organizations are in the process of developing internal documents.

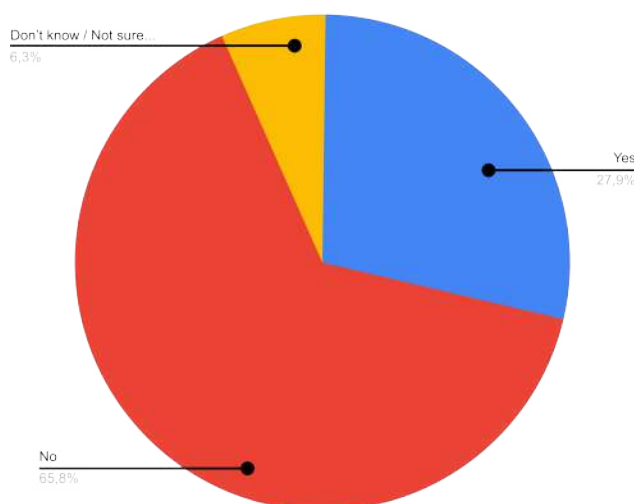
Does your organization have a policy/regulation/procedure for the collection, storage, and processing of personal data?



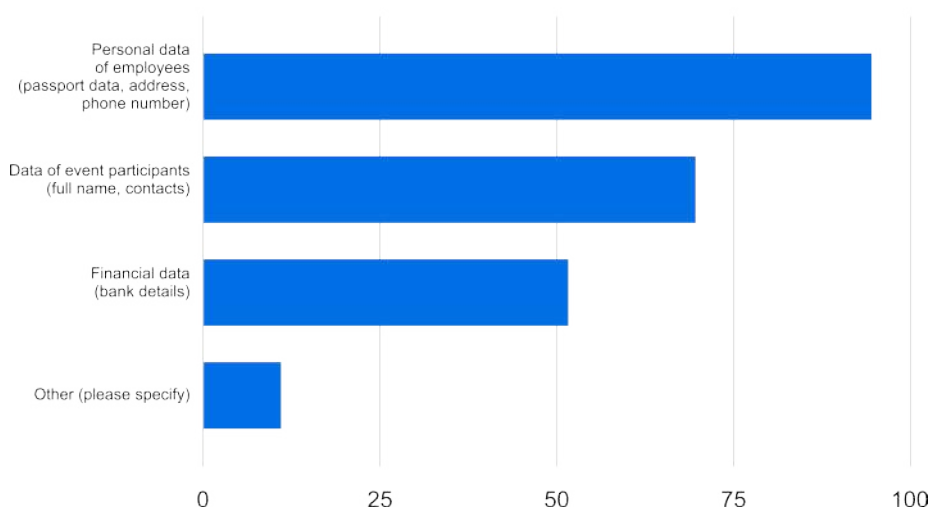


In addition, only 27.9 % of respondents indicated that their organization has appointed a person responsible for the processing and protection of personal data. And unfortunately, 65.8 % of respondents did not appoint a responsible person.

Is there a person responsible for the processing and protection of personal data in your organization?



What data does your organization collect and process?

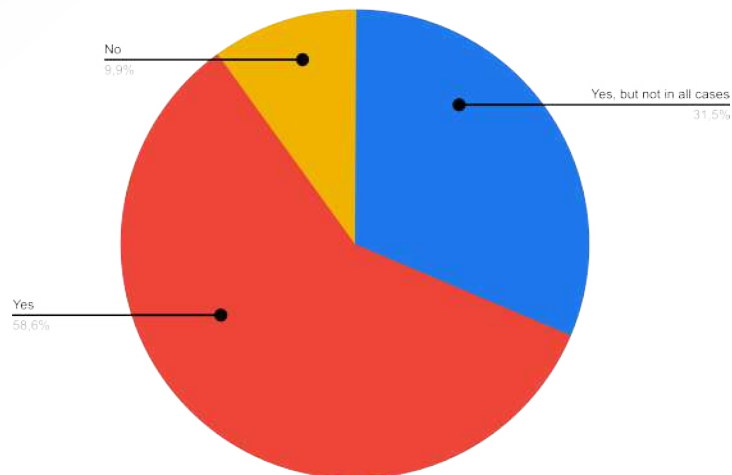


When asked what data or types of documents the organization collects, it turned out that most organizations collect and process personal data of employees (passport data, address, phone number). Next is the collection of data of event participants, in particular full name, contacts. And in third place is financial data (bank details). In the «Other» category, several respondents indicated such data as medical information, documents of other beneficiaries, information about



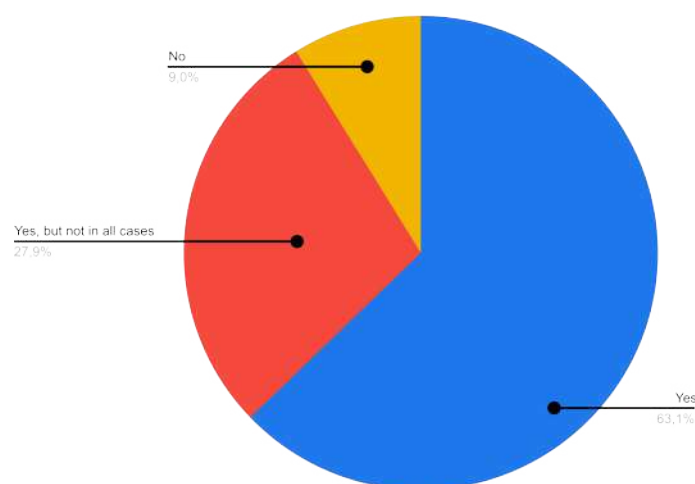
social programs. But at the same time, the survey showed that there are some organizations that noted that they do not collect personal data at all.

Do you obtain consent from the individual or their legal representative when collecting and processing personal data?



When asked whether the organization takes consent from an individual or their legal representative when collecting and processing personal data, 58.6% of respondents indicated that they take consent to process data, but 31.5% of respondents do not do this in all cases. And only 9.9% do not take consent.

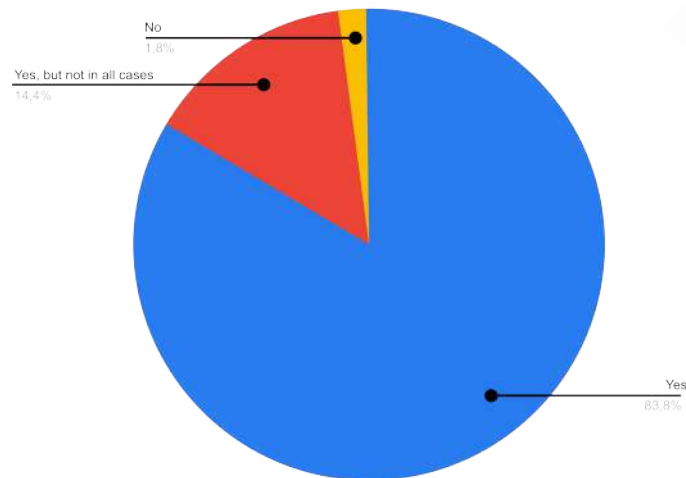
Do you define the purpose when collecting and processing personal data?



At the same time, the situation with defining the purposes of collecting and processing personal data showed that half of the respondents (63.1%) clearly formulate the purpose when collecting data. But 27.9% of respondents do not define the purpose in all cases.

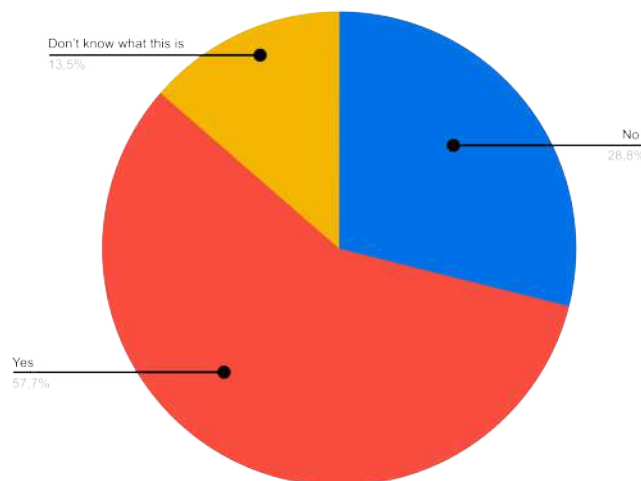


Are the collected personal data used only for the purposes initially stated?



A high rating of 83.8 % is shown by the answer to the question whether the collected personal data is used only for the previously stated purposes. Only 14.4 % do not always use the data for the previously stated purpose.

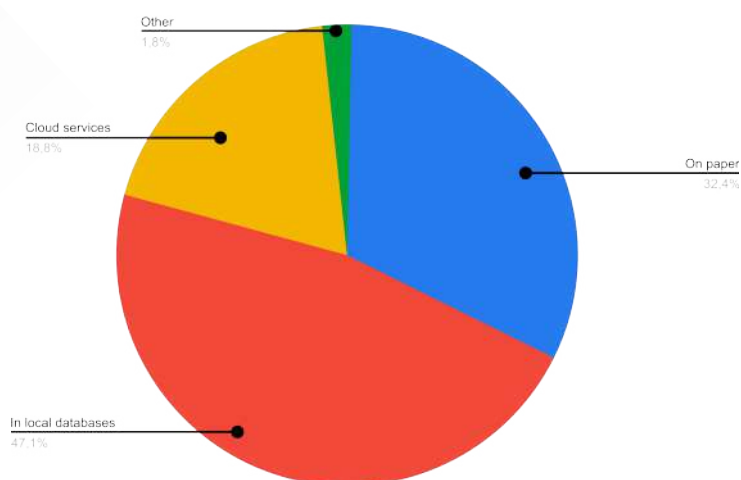
Do you classify personal data into public and restricted access categories?



When asked whether the organization separates personal data into publicly available and restricted access, it turned out that 57.7 % of respondents differentiate the data. And 28.8 % of respondents do not differentiate. But it should be noted that 13.5 % of respondents do not know what it is.

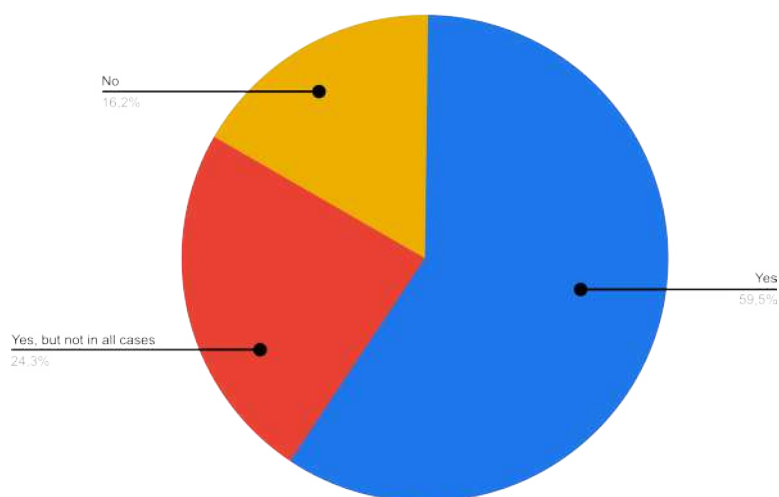
The survey showed that the storage of personal data occurs as follows: most organizations store data in local databases (47.1 %), store it on paper (32.4 %), and store it on cloud services (18.8 % of respondents).

How does your organization store personal data?



To what extent are protective measures applied to store personal data? The answers were distributed as follows: 59.5 % of respondents stated that they apply protective measures (in the form of passwords, encryption), but almost a quarter of organizations (24.3 %) do this irregularly, and 16.2 % do not use any protective measures at all.

Do you use protective measures for data storage?
(e.g., encryption, passwords)



It is important to note that in this survey, 10 organizations reported cases of possible leakage of personal data. Among the incidents mentioned were theft of hard drives, computers, use of the Pegasus program, publication of personal data on foreign Internet resources, and leakage of email passwords.

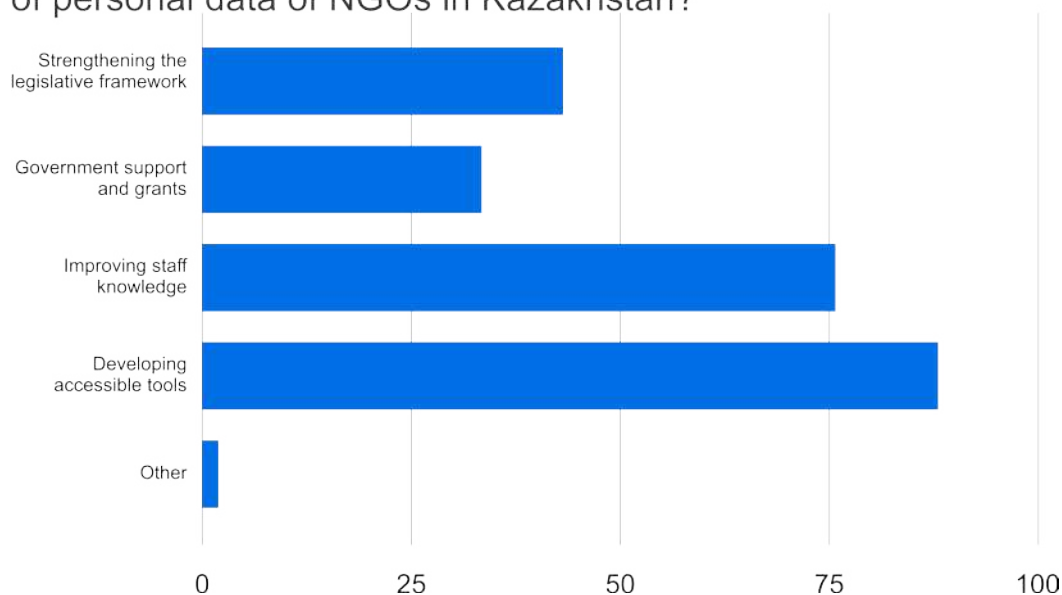


4.1 The fourth section of the survey was devoted to the difficulties and needs faced by the organization, as well as what measures are needed to protect personal data in public organizations.

So, to the question of what difficulties does an organization face in protecting personal data, the results of the answers show that the main difficulties that public organizations face in matters of protecting personal data are:

- lack of knowledge and skills among employees – 54.9 %
- limited financial resources to implement protective measures – 49.6 %
- lack of technical tools such as software or hardware – 46.9 %
- problems accessing legal or technical assistance – 36.3 %.
- lack of understanding of legal requirements – 33.6 %
- lack of interested or responsible employees – 29.2 %

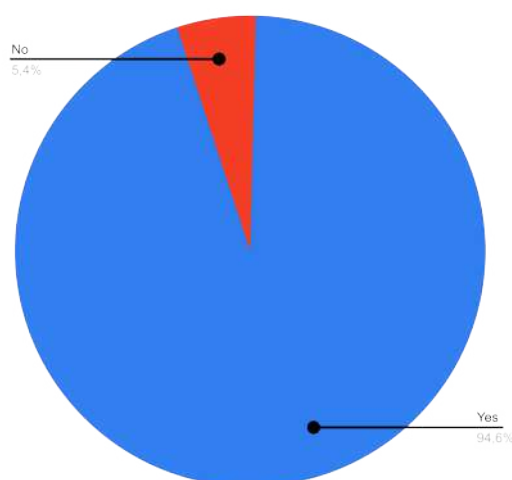
What measures, in your opinion, could improve the protection of personal data of NGOs in Kazakhstan?



When asked what measures could improve the protection of personal data of NGOs in Kazakhstan, the following measures were proposed:

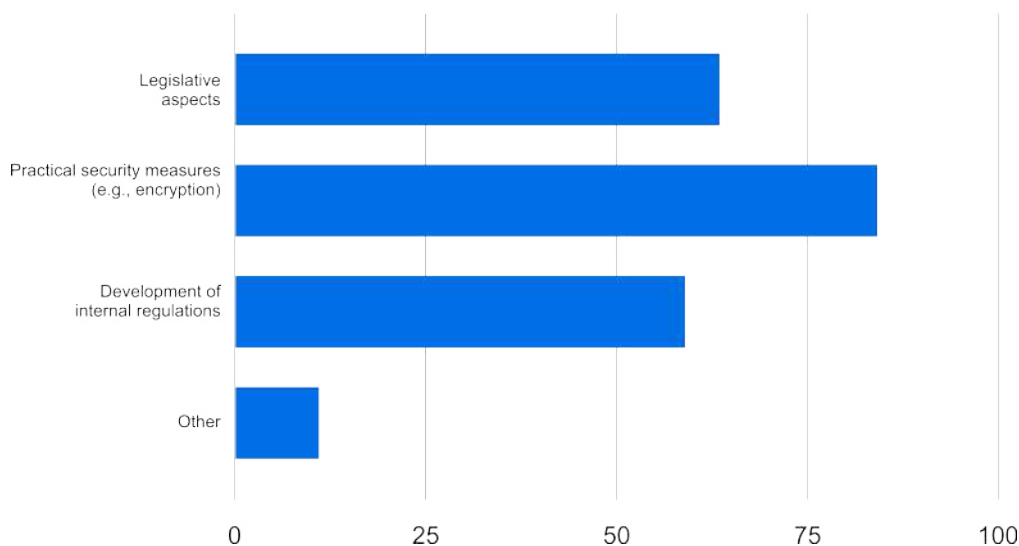
- The majority of respondents proposed the development of accessible tools for the protection of personal data;
- Next comes increasing the level of knowledge of employees of organizations;
- Strengthening the legislative framework;
- State support and grants.

Are you willing to participate in seminars or training on personal data protection?



It is especially necessary to note that there is a need to obtain knowledge on this topic, as evidenced by the respondents' answers. So, to the question «Are you ready to participate in seminars or trainings on the protection of personal data?» 94.6 % answered – Yes.

Which topics are most interesting to you for training in the field of data protection?



In the answers, the most interesting topics for training in the field of personal data protection were identified, such as:

1. Practical security measures (for example, encryption);
2. Legislative aspects;
3. Development of internal regulations;



ANALYSIS OF THE RESULTS OF FOCUS GROUPS ON THE PROTECTION OF PERSONAL DATA IN PUBLIC ORGANIZATIONS OF KAZAKHSTAN, CONDUCTED BY THE PF «ERKINDIK QANATY» IN FEBRUARY–MARCH 2025

In addition to the questionnaire, 5 focus groups were held as part of the study (2 were held offline in Astana and 3 focus groups online).

Representatives of 29 public organizations from 9 regions of Kazakhstan participated in the focus groups: Astana, Almaty, Turkestan region, Ust–Kamenogorsk, Pavlodar, Uralsk, Semey, Atyrau and Taraz.

The purpose of the focus groups was to conduct a more in–depth analysis of the practices and difficulties associated with the processing of personal data, as well as to verify and clarify the results of the online survey.

During the discussions, most of the conclusions obtained through the questionnaire were confirmed, and also supplemented with context, which shows the approaches to personal data used by non–profit organizations in practice, as well as cases from work.

Just as in the survey, most of the focus group participants were human rights activists, but there were also organizations whose activities were aimed at research, creative projects, ecology and other areas.

Thematic analysis is used for analysis, identifying certain similarities or differences in the work of different organizations.

THE RESULTS OF THE FOCUS GROUP

1. Personal data handling policies

As the results of both the survey and focus groups showed, most public organizations do not have separate, formalized policies or regulations devoted to handling personal data.

At the same time, during the discussions it became clear that individual elements of such policies are still present in other internal documents of organizations. For example, in some cases, non–disclosure agreements on personal data are concluded when drawing up contracts with employees, and consents to data processing are



also used when collecting them. Some organizations have provisions regarding handling personal data spelled out as part of internal procedures, for example, in documents on working with beneficiaries or when organizing events.

Quotes from respondents' answers

«We used to request a copy of the ID card to keep in the documentation. Since the legislation has changed, we stopped doing this. And now we simply ask people to either write us the ID card data or fill it out in the contract themselves. That is, we no longer attach any copies of ID cards to the contracts.» (Almaty)

«Most non-profit organizations in Kazakhstan are quite compact [...] with a staff of two or even one person. On average, the headquarters of a non-profit organization is 3–5 people. It is important to understand for whom these policies are written. That is, policies are appropriate when there are some serious business processes and communications within the framework of working relationships. And in the context of most organizations in the non-profit sector, the appropriateness of most policies in many cases seems optional. For example, we are forced to make a personnel management policy. What kind of personnel management, if the personnel consists of a director, an accountant and a coordinator? But what kind of personnel management, if all this can be regulated by job descriptions, which are an appendix to individual employment contracts?» (Almaty)

«Since we are required to store all primary financial documentation for tax purposes for 10 years, for pension purposes for life, everything that concerns the staff, we naturally archive all of this. Archiving occurs according to certain rules and requirements. All of this is stored in the office under three locks. In electronic form, primary documentation is stored with us only if we send some scan of financial statements to our donors. And all of this is also archived. In cloud storage format, but it is stored exactly as long as required by the donors themselves. This can be 3, 5, 10 years, standard storage periods.» (Ust-Kamenogorsk).

Among those who have implemented full-fledged policies, two main groups can be distinguished. The first are organizations that **have adopted such documents within the framework of donor requirements** (mainly foreign). The second are those who **have developed and implemented the policy after completing training programs** and use it in everyday practice, realizing its importance. At the same time, representatives of both groups note that in practice, compliance with all provisions of the document is extremely difficult. The main reasons are: lack of time, human resources and limited organizational capabilities, which is especially typical for small public organizations with a limited budget aimed only at implementing projects.



2. Lack of a systematic approach

The second key feature of personal data practices in public organizations follows from the previous section – the lack of a systematic approach, primarily due to limited resources and the difficulty of understanding legal requirements. Almost all organizations take certain actions to protect data. For example, they use secure storage locations (e.g., metal safes), delete personal data after the end of projects, use two-factor authentication, complex passwords, and include consent notes when collecting data through online forms. However, these measures are not systematic and are often implemented without a single strategy or coordination. In the context of public organizations, when several people in the organization can combine different functions and the main focus is on the implementation of project activities, data protection issues do not receive due priority.

Moreover, despite familiarization with the Law «On Personal Data and Their Protection», respondents note a lack of understanding of the practical application of legal requirements and a lack of clarification from authorized bodies. Organizations lack adapted explanations, instructions and examples that would take into account the specifics of their activities and the real possibilities of implementing the standards in practice.

3. Working with donors

«We always have this question about transferring data to the donor, because we cannot guarantee the safety of this data with the donor, be it a foreign organization, an international or state organization [...] And the requirements go all the way down to copies of documents.» (Ust-Kamenogorsk).

One of the important aspects raised during the focus groups was the topic of interaction with donors, especially in the context of transferring personal data of beneficiaries. The specifics of the work of non-profit organizations are closely related to working with donors, both international and state, and mandatory reporting to them.

In some cases, to confirm the implementation of the project, the services rendered and the development of the budget, donors request not only publicly available data such as full names, but also sensitive information, including copies of documents, certificates of diagnoses, information on social statuses and others.

Organizations can ensure data protection within their structure. However, after the data is transferred to the donor, control over further use and storage becomes impossible.

The problem is especially acute when working with government grants regulated by the Center for Support of Civil Initiatives (CSCI). As respondents note, the texts of grant agreements often directly indicate the requirement to transfer personal



data of project participants, including their full names, contact details, and other information. For public organizations, this creates a conflict between the legal obligation to transfer data and the responsibility for its protection. Moreover, during the discussions, cases emerged where, several years after the completion of the project, beneficiaries received calls from government representatives with questions about their participation in the projects, which may indicate long-term storage of data in structures not controlled by non-profit organizations.

4. Responsibility of state bodies

During the focus groups, a persistent feeling of anxiety was revealed among representatives of non-profit organizations related to working with personal data. In addition to a lack of knowledge and resources, this is also due to mistrust on the part of beneficiaries and a potential threat from government agencies, including hacking of internal systems and checks. Many organizations note that more and more beneficiaries are afraid to provide personal data in the context of increased cases of cyber fraud. This is especially noted in projects where work is carried out with elderly groups. At the same time, there is a fear that government agencies can gain access to internal data of organizations. Participants shared cases where such interference had already occurred. Thus, a respondent from the city of Taraz described a situation when an expert who received a fee received calls from the police with questions about their activities. There was no transfer of data from the organization, and, in the participant's opinion, the source of such information could only be government or banking systems.

Quote from the respondent's answer

«All beneficiaries who received fees from the organization received calls from third parties, from police officers, from the bank, even from the National Security Committee. And what was already said above, that the first threat is from the state. I want to confirm this from my personal experience, since no one except me has any information. I myself keep the organization's accounting, that is, the drain was only from my report to the tax committee, or from the bank, from managers who see the state of accounts and the amounts in the accounts.» (Taraz)

This creates a feeling of insecurity even in cases where the organization complies with all legal requirements. As a result, the topic of data protection is perceived not only as a technical and legal issue, but also as a factor in the security of the organization itself.



It is important to note that without legislative grounds, government agencies do not have the right to demand personal data of employees of organizations.

The collection and processing of personal data is carried out only with the consent of the subject or his legal representative, with the exception of certain cases. At the same time, the collection and processing of personal data, including their use, must be carried out only within the framework of the purposes established by the operator. At the same time, the operator must draw up a clear and specific list of the necessary personal data that are necessary to achieve the established purpose.

Those individual cases when the consent of the subject or his legal representative for the collection and processing of personal data is not required are enshrined in Article 9 of the Law «On Personal Data and Their Protection».

In this described answer of the respondent, this is in the case of the activities of law enforcement agencies, courts and other authorized state bodies that initiate and consider cases of administrative offenses, enforcement proceedings. But it should be noted that these cases must be in production, under investigation, and also in connection with the inspection.

5. Organizations' needs and recommendations for sustainable work with personal data

An analysis of surveys and focus groups showed that public organizations in Kazakhstan face not only resource constraints, but also a lack of systemic, understandable, and accessible support in matters of working with personal data. These limitations concern both the internal capabilities of organizations and regulation.

One of the most expressed needs of organizations was accessible training on legislation, including new by-laws, as well as consultations and support on law enforcement.

Representatives of the public organization emphasize that familiarization with the law is not enough; a «translation» of the norms into the language of practice is needed: understandable materials, visual guidelines, instructions, and memos, especially designed for non-lawyers. For example, online courses, mini-lectures with step-by-step actions that are always available.

An important proposal was the creation of automation tools, for example, a Telegram bot that generates consent templates, policies, and reminds about the need to delete data. Many emphasize that in the conditions of a lack of



resources, both financial and personnel, public organizations cannot afford lawyers or dedicated departments. Therefore, the idea of outsourcing or standard solutions for the sector is especially relevant. Existing business practices, where there are ready-made products, could be adapted for the non-profit sector.

A separate block of recommendations concerns the legislative and institutional environment. Focus group participants emphasize that:

- It is necessary to reduce sanctions, especially in relation to non-profit organizations, and avoid repressive approaches.
- It is important not only to punish, but also to encourage compliance with standards, with bonuses, priorities in competitions and recognition.
- Laws must be made clear, unambiguous, not subject to arbitrary interpretation. Now they are interpreted differently, which creates legal uncertainty.
- It is necessary that independent experts and representatives of public organizations, and not only government agencies, participate in the development of standards.
- The state should set an example: with constant leaks from government agencies (which is publicly acknowledged), trust in requirements is lost.
- The role of the state should not only be regulating, but also supporting. Public organizations want to see a real reaction from the state, transparent communication channels, centralized resources, as well as clear appeal algorithms and the ability to receive prompt assistance, including a hotline and accessible legal support.



CHALLENGES AND RISKS RELATED TO PERSONAL DATA PROTECTION IN PUBLIC ORGANIZATIONS


The results of the questionnaire and survey revealed similar practical problems and risks in the area of personal data protection. Many respondents spoke about the importance of protecting personal data, but there were others who did not fully understand the meaning of the Law on the Protection of Personal Data and their Protection.

In general, the survey was of a general nature, since the study aimed to understand how things are with the security of personal data protection in public organizations.

At the same time, it turned out that representatives of public organizations are mostly familiar with the Law «On Personal Data and Their Protection» and are interested in raising the level of awareness on these issues.

Based on the survey, the following are proposed as the main challenges and threats in the area of personal data:

- 1. Innovative technological changes:** The rapid growth of technologies, including cloud solutions and mobile applications, and other innovations create new requirements for the processing and protection of personal data.
- 2. Frequently changing laws, regulations:** Amendments and additions to regulatory legal acts require periodic updates of internal policies and procedures for the protection of personal data.
- 3. Lack or shortage of knowledge and skills:** Personal data subjects usually do not understand to whom, why and in what volume they transfer their personal data. This leads to gaps in the field of legal support for the protection of personal data, to difficulties in complying with current legislation by organizations. It is necessary to provide personnel with sufficient knowledge in the field of personal data protection. Often, employees are not aware of the risks associated with the processing of personal data.
- 4. Limited resources:** Public organizations do not have sufficient financial resources to implement modern security systems, attract a separate specialist in the protection of personal data, and train employees.
- 5. Lack of self-control:** Personal data subjects do not monitor further actions in relation to their personal data. Which in turn would minimize the risks of unlawful use of data.

-
- 
6. Accidental or intentional copying of documents, disclosure of information due to accidental or intentional printing.

In addition, it is proposed to highlight some risks that may cause harm to both the owner of personal data and public organizations:

1. **Data leakage.** Improper handling of data can lead to its leakage, which can cause serious damage to both organizations and individuals whose data has been disclosed. Information leakage channels are: removable media, e-mail, paper documents, desktop computers, mobile equipment.
2. **Unauthorized access to databases,** associated with the vulnerability of software services and support, as well as the human factor.
3. **External threats** (cyberattacks, phishing, malware, etc.). In particular, public organizations can become a target for hackers, especially if they do not have appropriate security measures.
4. **Internal threats** (employee errors, lack of awareness of the legislation in this area, etc.).
5. **Lack of control:** The lack of constant control over software updates and the systems used to store and process data may be unsatisfactory or outdated, which increases the risk of leaks and attacks.
6. **Fraud or misuse of personal data.** Any kind of manipulation, deceptive ways of gaining trust can provoke fraudulent actions.
7. **Violation of legislation:** In case of failure to comply with the rules and requirements for data protection, this can lead to significant fines. This risk will negatively affect the activities of a public organization, up to and including suspension.
8. **Low level of digital literacy.** Among the population, there is still a significant number of citizens who do not have the skills to work with data and technology. And this can be reflected in the effective use of data, as well as in the collection, processing and storage of data.

In this regard, systematic work is needed to overcome these challenges and risks, a comprehensive approach is required. Starting with staff training, improving the institutional system within the organization, developing a policy and strategy for managing personal data and the active participation of all stakeholders.



RECOMMENDATIONS


In order to respect human rights, protect personal data, and avoid risks, breaches of confidentiality, and violations of legislation in the field of personal data protection, it is necessary to take appropriate measures.

The survey showed that representatives of public organizations have a poor understanding of what measures, policies, and documents need to be taken in the organization.

In this regard, **it is recommended:**


Public organizations shall develop practical tools in the organization in the form of the following types of documents:

1. **Policy for the protection and processing of personal data.** This document shall be developed based on the provisions of the Law, as well as the specifics or type of activity of the organization.
2. **Regulation on the personal data of employees.** The document shall be based on the provisions of the Labor Code of the Republic of Kazakhstan, including the right to familiarize oneself with the text of the Employee Regulation.
3. **Regulation on the procedure for maintaining personal files of employees,** rules for processing, storing and transferring personal data of employees contained in personal files
4. **Development and implementation of a privacy policy.** The document shall clearly and specifically define what information the organization collects, how it will be used and who will have access to it.
5. **Form of consent to the processing of personal data,** based on the Law «On personal data and their protection»
6. **Development of an Employee Training Program.** Conduct regular training on personal data protection to raise awareness of best practices and ways to prevent information leaks.
7. **Development of an encryption program for data protection and storage.** Involve a specialist to develop the program.
8. **Employer's regulations for conducting regular audits and inspections** with the involvement of a specialist to identify vulnerabilities and eliminate them in a timely manner.

- 
9. **Regulation on the storage of personal data.** Include the storage period for personal data and their deletion due to the exhaustion of the purpose of collection and storage.
 10. **Employer's regulations for compliance with legislation in the field of personal data protection.** Study national and international legislation on the protection of personal data. Minimize the risks associated with their leakage or illegal use.
 11. **Vulnerability analysis.** Regular penetration testing and vulnerability analysis in data processing systems.
 12. **Informing.** Creation of information materials (brochures, memos, internal mailings) on the principles of processing and protecting personal data.
 13. **Regular analysis of current practices** will allow organizations to comply with legal requirements, increase the trust of customers and partners.
 14. **Order on the appointment of a specialist** responsible for working with personal data.

Only a few survey participants were able to answer questions related to state regulation of personal data protection and, in particular, the question of which state body is the authorized body in this area. At the same time, given that the relevant Law contains gaps in the regulation of certain social relations, the following recommendations are offered:

2. **To the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan**
 1. Development of common standards and guidelines for processing personal data taking into account the needs of public organizations.
 2. Organization and holding of round tables with the participation of representatives of public organizations, government agencies in the field of personal data protection.
 3. Development of specialized programs for providing legal and advisory assistance to public organizations on issues of personal data protection.
 4. Organization and holding of training seminars, trainings for representatives of public organizations to explain the legal norms of personal data protection.
 5. Development and adoption of the Rules for notifying personal data subjects about actions with their personal data.

- 
6. Development and adoption of the Rules for the destruction of personal data upon expiration of the purpose of use. The absence of a clear procedure may create ambiguity when independently implementing this procedure.
 7. Development and adoption of the List of criteria that must be met when agreeing to the collection and processing of personal data (for example, voluntariness, lack of coercion, awareness, etc.). The current Law does not have a list of criteria.

Comments to paragraph 7

The lack of a clear definition of what a publicly available source is may violate the rights of the personal data subject.

For example, a publicly available source may contain information that the personal data subject did not intend to disclose. Also, combining personal data from various publicly available sources may lead to an incorrect idea of a person, which may negatively affect their reputation or other aspects of life and other potential situations. Or the use of inaccurate or outdated personal data previously published in publicly available sources may lead to incorrect conclusions about a person, which may also be a violation of the rights of the subject.

There is a response from the Information Security Committee of the Ministry to the applicant's question: *«Is it permissible to classify any online platform or other source containing publicly available information, i.e. information that cannot be limited by law or that is disclosed (distributed) by the person (natural or legal) himself as publicly available?»* The Committee answers that **«...social networks are permissible to classify as publicly available sources.»**

However, according to Article 60 of the Law «On Legal Acts», **such explanations do not have binding legal force and are advisory in nature.**

8. Introduce the term «publicly available source» into the conceptual apparatus, since this phrase is used in Article 7 of the Law.
9. Clarify the conditions for repeated collection, processing and distribution of personal data by third parties, since the current Law does not contain a requirement for consent for repeated collection. (clauses 3, 4 of Article 7 of the Law).



CONCLUSION

Particularly relevant now are the aspects of protecting, collecting, processing and storing personal data by organizations when hiring employees, the intricacies of exchanging personal data when concluding contracts, protecting personal data on the Internet, as well as issues of storing and destroying personal data.

In addition, public organizations working in various fields, from health care to education and social assistance, have special obligations to ensure the confidentiality and security of the data of their participants, volunteers and clients.

By developing an effective management strategy in the field of protecting personal data from fraud, misuse of data, it is possible to achieve a balance between the use of technology to optimize work and the protection of citizens' rights to the privacy and security of their data.

Proper and competent management of personal data protection will prevent data leakage, strengthen trust on the part of stakeholders, which is a key aspect of the sustainable development of any organization.

Public organizations should actively consider the risks and challenges associated with the protection of personal data and develop strategic approaches to minimize them.

Today, there are many tools and methods for ensuring the security of personal data, among which are encryption, the use of an access control system, regular audits and employee training.

It is important to note that the human factor often plays a decisive role in security issues, so training and raising employee awareness of risks and protection methods should become a priority for every public organization.

I would especially like to draw attention to the key actions to achieve the goal of ensuring the security of personal data in organizations:

1. Security Policy
2. Risk Assessment
3. Employee Training
4. Technical Protection Measures
5. Monitoring and Response



It is also necessary to consider the need to comply not only with national legislation but also with data protection standards, such as GDPR. This will not only help to avoid legal consequences, but will also be the key to a good reputation and competitiveness of the organization.

Public organizations need to take the initiative to improve legislation on the protection of personal data. These initiatives will further create a safe environment for the processing of personal information.

Thus, the comprehensive implementation of measures to improve the security of personal data in public organizations is not just a necessity, but also a strategic choice for stability in the rapidly changing digital environment.

The protection of personal data in public organizations is not just a legal obligation, but also an important aspect of their social responsibility.

It should be noted that raising public awareness of the protection of personal data and digital rights will create a sustainable ecosystem in society.

Successful implementation of data protection measures will contribute not only to compliance with the law, but also to the formation of public organizations as reliable and open institutions that contribute to the development of civil society.



REFERENCES

1. Universal Declaration of Human Rights, Adopted by General Assembly resolution 217 A (III) of 10 December 1948.
2. International Covenant on Civil and Political Rights, Adopted by General Assembly resolution 2200A (XXI) of 16 December 1966.
3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the member states of the Council of Europe on January 28, 1981.
4. The Constitution of the Republic of Kazakhstan, adopted at the republican referendum on August 30, 1995.
5. Law of the Republic of Kazakhstan "On Personal Data and Their Protection" dated May 21, 2013, No. 94–V.
6. <https://kapital.kz/tehnology/128514/v-rk-rastet-chislo-pravonarusheniy-svyazannykh-s-zashchitoy-personal-nykh-dannykh.html>
7. <https://liter.kz/v-kazakhstane-proveli-proverki-na-12-mln-tenge-v-sfere-zashchity-personalnykh-dannykh-1742455826/>
8. <https://www.gov.kz/memleket/entities/inf/activities/142>



INIDI

ERKINDIK
QANATY
общественный фонд

INSTITUTE FOR
WAR & PEACE REPORTING
I W P R
ИНСТИТУТ РЕПОРТАЖЕЙ ВОЙНЫ И МИРА