Document approved by: JSC I.T.M.S.
Order No. 43/1-r dated 03/29/2024

Date for the implementation: 1 April 2024

POLICY

**Joint-stock company**

**"I.T.M.S."**

**regarding the processing of personal data**

**and information on the requirements being implemented**

**to the protection of personal data**

# 1. General Provisions

* + 1. This Policy (hereinafter referred to as **the Policy** ) defines the general principles and procedure for processing personal data and measures to ensure their security in the Joint Stock Company "I.T.M.S." (hereinafter referred to as **the Company** ).
		2. The purpose of the Policy is to ensure the protection of the rights and freedoms of a person and citizen when processing his personal data, including the protection of the rights to privacy, personal and family secrets, strict and strict compliance with the requirements of the legislation of the Russian Federation and international treaties of the Russian Federation in the field of personal data.
		3. The policy has been developed in accordance with the provisions of the Federal Law of 27.07.2006 No. 152-FZ "On Personal Data", other legislative and regulatory legal acts (hereinafter referred to as legislation), determining the procedure for working with personal data and requirements for ensuring their security.
		4. The following terms are used in the Policy:

**automated processing of personal data** – processing of personal data using computer technology;

**personal data base** – an ordered array of personal data, independent of the type of material carrier of information and the means of its processing used (archives, card files, electronic databases);

**biometric personal data** – information that characterizes the physiological and biological characteristics of a person, on the basis of which his identity can be established and which is used by the operator to establish the identity of the subject of personal data;

**blocking of personal data** – temporary cessation of processing of personal data (except in cases where processing is necessary to clarify personal data);

**data center** – a specialized organization providing services for the placement of server and network equipment, leasing of servers (including virtual ones), and also for connecting to the Internet;

**access to personal data –** familiarization of certain persons (including employees) with the personal data of subjects processed by the Company, subject to maintaining the confidentiality of this information;

**personal data information system** – a set of personal data contained in databases and the information technologies and technical means that ensure their processing;

**use of personal data** – actions (operations) with personal data performed by the operator for the purpose of making decisions and/or performing other actions that generate legal consequences in relation to the subject of personal data or other persons, or otherwise affect the rights and freedoms of the subject of personal data or other persons;

**counterparty** – a party to an agreement with the Company that is not an employee of the Company;

**confidentiality of personal data** – the obligation of persons who have gained access to personal data not to disclose it to third parties and not to distribute personal data without the consent of the subject of the personal data, unless otherwise provided by law;

**Cloud computing infrastructure is** a shared pool of configurable computing resources (data networks, servers, storage devices, applications, and services, either individually or collectively) that are widely and conveniently accessible over the network on demand and that can be quickly provisioned and released with minimal operational costs or service provider requests, and that have five key properties: on-demand self-service; universal network access; resource pooling; elasticity; consumption metering;

**processing of personal data** – any action (operation) or set of actions (operations) performed with the use of automation tools or without the use of such tools with personal data, including collection, recording, systematization, accumulation, storage, clarification (updating, modification), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of personal data;

**publicly available personal data** – personal data, access to which by an unlimited number of persons is granted by the subject of personal data either at his request or on the basis of his consent, as well as data that are subject to mandatory disclosure or publication in accordance with federal law;

**operator** – a state body, municipal body, legal entity or individual that independently or jointly with other persons organizes and (or) carries out the processing of personal data, and also determines the purposes of processing personal data, the composition of personal data subject to processing, actions (operations) performed with personal data; in the Policy, the operator means the Company, unless otherwise specifically indicated;

**personal data** – any information relating to a directly or indirectly identified or identifiable individual (subject of personal data);

**personal data permitted by the subject of personal data to be distributed** – personal data, access to which by an unlimited number of persons is granted by the subject of personal data by giving consent to the processing of personal data permitted by the subject of personal data to be distributed in the manner prescribed by the Federal Law “On Personal Data”;

**provision of personal data** – actions aimed at disclosing personal data to a specific person or a specific group of persons;

**dissemination of personal data** – actions aimed at disclosing personal data to an indefinite number of persons;

**Roskomnadzor** is the Federal Service for Supervision of Communications, Information Technology and Mass Media, which is entrusted with the functions of the authorized body for the protection of the rights of personal data subjects, as well as the functions of federal state control (supervision) over the compliance of personal data processing with the requirements of the legislation of the Russian Federation in the field of personal data;

**special categories of personal data** – information relating to race, nationality, political views, religious or philosophical beliefs, health status;

**subject of personal data** – an individual to whom the personal data relates;

**cross-border transfer of personal data** **–** transfer of personal data to the territory of a foreign state to a foreign government body, a foreign individual or a foreign legal entity;

**destruction of personal data** – actions as a result of which it becomes impossible to restore the content of personal data in the personal data information system and (or) as a result of which the material carriers of personal data are destroyed;

# The status of the Company and categories of subjects whose personal data are processed by the Company

* 1. The Company is the operator in relation to the personal data of the following categories of individuals:
* employees of the Company with whom the Company has concluded or has concluded employment contracts, including former employees with whom employment contracts have been terminated (discontinued) (hereinafter referred to as **Employees** );
* close relatives, spouses of employees of the Company and persons dependent on employees, including former spouses to whom alimony is paid (hereinafter referred to as **Family Members of Employees** );
* employees of the Joint Stock Company “International Tobacco Marketing Services” and employees of other legal entities affiliated with JSK “I.T.M.S.” (hereinafter referred to as the Employees of the Group of Companies);
* applicants for vacant positions of the Company (candidates for employment by the Company) who have submitted their resumes or applications containing personal data, in person or through specialized personnel selection organizations (recruitment agencies), including through specialized websites on the Internet, and in relation to whom the Company has taken the initiative to hire (hereinafter referred to as **Applicants** );
* counterparties who are individuals and sole proprietors, representatives of counterparties who are legal entities and sole proprietors , including employees, owners, including beneficial owners, representatives acting on the basis of a power of attorney and other representatives of counterparties with whom the Company has contractual relations, with whom the Company intends to enter into contractual relations or who intend to enter into contractual relations with the Company (hereinafter referred to as **Representatives of Counterparties** );
* representatives of personal data subjects who are not employees of the Company and who apply to the Company on behalf of and on behalf of personal data subjects (hereinafter referred to as **Representatives of** **personal data subjects** );
* visitors to the Company’s protected premises who do not have the right of permanent entry into such premises (hereinafter referred to **as Visitors** );
	1. The company is the person providing the services personal data to other operators, which include (without limitation):
* authorities and local governments, state extra-budgetary funds to which information is provided and funds of Employees are transferred or funds are credited to the accounts of Employees (the Ministry of Internal Affairs of Russia in relation to highly qualified foreign workers, inspectorates of the Federal Tax Service, territorial offices of the Social Fund of Russia, the Federal Compulsory Medical Insurance Fund, etc.), supervisory authorities;
* statistical authorities and other competent bodies to which this information must be provided in accordance with the legislation of the Russian Federation;
* communications operators who are provided with information about users of corporate communications services (fixed and mobile telephony, Internet access) in accordance with legal requirements.
	1. Personal data is provided (transferred) to authorities and state extra-budgetary funds, communications operators and other bodies specified in paragraph 2.2 in the volume determined by legislation, by the relevant authorities, state extra-budgetary funds and organizations. within the limits of their authority. The consent of the subjects for such transfer of personal data is not required.

# Principles of personal data processing

The processing of personal data by the Company is carried out in accordance with the following principles:

* 1. Legality and fair basis for processing personal data. The Company takes all necessary measures to comply with the requirements of the law, does not process personal data in cases where this is not permitted by law and is not required to achieve the goals determined by the Company, does not use personal data to the detriment of the subjects of such data.
	2. Limitation of personal data processing to the achievement of specific, predetermined and legitimate purposes. The purposes of personal data processing by the Company are:
* **in relation to Employees** - compliance with labor legislation, performance of the functions, powers and duties imposed by law on the Company as an employer, including assistance in employment, training and career advancement, ensuring the personal safety of employees, monitoring the quantity and quality of work performed, maintaining personnel and accounting records, ensuring the safety of property; calculation and payment of wages, other remuneration, calculation and transfer of taxes and insurance premiums; provision of additional services to Employees at the expense of the employer (transfer of income to employee payment cards, insurance at the expense of the employer, non-state pension provision, travel support, visa support, providing the opportunity to rent housing and use a rented (leased) corporate car through the company's counterparties, consulting on tax issues, provision of educational services, provision of a parking space), ensuring the possibility of the Employee transferring charitable donations;
* **in relation to Family Members of employees** – provision of benefits and guarantees to Employees stipulated by legislation and documents of the employer (insurance of Family Members of employees partially or fully at the expense of the Company, provision of educational services, consultation on tax issues); compliance with the requirements of the Labor Code of the Russian Federation on informing relatives about accidents;
* **in relation to Employees of the group of companies –** personnel administration, including maintaining personnel records, issuing payment cards for accrual of income, providing insurance for Employees of the group of companies, monitoring compliance with legislation and internal procedures of the group of companies;
* **in relation to Applicants** – selection and hiring of personnel ;
* **in relation to Representatives of counterparties** – compliance with the provisions of the Civil Code of the Russian Federation governing contractual work, the conclusion and execution of contracts with counterparties;
* **in relation to Representatives of personal data subjects** – the performance by the Company of actions on behalf of Representatives of personal data subjects ;
* **in relation to Visitors** – ensuring the possibility of entry into the guarded premises of the Company for persons who do not have permanent passes, monitoring their departure from the guarded premises, providing the possibility of parking on the territory of the Company;
	1. Processing only those personal data that meet the previously declared purposes of their processing; compliance of the content and volume of the processed personal data with the declared purposes of processing; prevention of processing of personal data that is incompatible with the purposes of collecting personal data, as well as excessive in relation to the declared purposes of processing personal data. The Company does not collect or process personal data that is not required to achieve the purposes specified in paragraph 3.2 of the Policy, does not use the personal data of subjects for any purposes other than those specified.
	2. Preventing the merging of databases containing personal data, the processing of which is carried out for purposes that are incompatible with each other.
	3. Ensuring the accuracy, sufficiency and relevance of personal data in relation to the purposes of personal data processing. The Company shall take all reasonable measures to maintain the relevance of the personal data being processed, including (without limitation) the exercise of the right of each subject to receive their personal data for review and to require the Company to clarify, block or destroy them if the personal data are incomplete, outdated, inaccurate, illegally obtained or are not necessary for the above-stated purposes of processing without explaining the reasons for such a requirement .
	4. Storage of personal data in a form that allows the identification of the subject of personal data for no longer than required by the purposes of processing personal data, unless the storage period of personal data is established by law, an agreement to which the subject of personal data is a party, or the consent of the subject of personal data to the processing of data.
	5. Destruction of personal data upon achievement of the stated purposes of their processing or in the event of loss of the need to achieve these purposes, if the Company is unable to eliminate the violations committed by the procedure for processing personal data established by law, withdrawal of consent to the processing of personal data by the subject, expiration of the period for processing personal data established by local acts of the Company, consent to the processing of personal data, unless otherwise provided by law or agreements with subjects of personal data.
	6. When processing personal data, the Company assumes that subjects provide reliable information about themselves and does not assume any obligations to verify the personal data received, although it reserves the right, if necessary, to perform such verification by legal means, including verification of the age of Users of the sites.

# Terms of personal data processing

* 1. The processing of personal data by the Company is permitted in the following cases:
1. If the personal data subject has consented to the processing of his/her personal data. The procedure for obtaining the consent of the personal data subject by the Company is defined in Section 7 of the Policy.
2. The processing of personal data is necessary for the implementation and performance of the functions, powers and obligations imposed on the Company by law.
3. To conclude an agreement on the initiative of the personal data subject and to execute an agreement to which the personal data subject is a party. Such agreements include, without limitation, employment contracts with Employees, user agreements on the Company's websites on the Internet.

Until the conclusion of the said agreements, the Company processes personal data at the stage of pre-contractual work in the selection of personnel, when the subject's consent to the processing is confirmed by the Applicant's personally completed questionnaire or questionnaire (resume) submitted by him to the Company or to a specialized organization for the selection of personnel, or posted by the Applicant on specialized websites on the Internet, or sent by the Applicant to the Company by e-mail.

An agreement concluded with a personal data subject may not contain provisions that limit the rights and freedoms of the personal data subject, establish cases of processing the personal data of minors, unless otherwise provided by the legislation of the Russian Federation, as well as provisions that allow inaction of the personal data subject as a condition for concluding an agreement.

1. The processing of personal data by the Company is necessary for the exercise of the rights and legitimate interests of the Company and/or third parties or for the achievement of socially significant goals, provided that the rights and freedoms of personal data subjects are not violated.
2. The processing of personal data is carried out for statistical or other research purposes, subject to mandatory anonymization of personal data.
3. Processing of personal data, access to which is granted to an unlimited number of persons by the subject of personal data by giving consent to the processing of personal data, permitted by the subject for distribution.
4. Personal data is subject to publication or mandatory disclosure in accordance with the law.
	1. The Company does not disclose to third parties or distribute personal data without the consent of the personal data subject, unless otherwise provided by law, an agreement with the personal data subject, or specified in the consent received from him for the processing of personal data, or the personal data are made publicly available by the subject independently.
	2. The Company does not process personal data related to special categories and concerning racial and national affiliation, political views, religious or philosophical beliefs, intimate life (except for information about the state of health related to the issue of the possibility of the Employee performing a work function and necessary for the purposes determined by the legislation on state social assistance, legislation on compulsory types of insurance, labor, pension and insurance legislation), about the membership of personal data subjects in public associations or their trade union activities, except for cases expressly provided for by law.
	3. The processing of personal data on criminal records is carried out by the Company exclusively in cases and in the manner established by law.
	4. The Company does not process biometric personal data.
	5. When collecting personal data, the Company ensures the recording, systematization, accumulation, storage, clarification (updating, modification), and extraction of personal data using databases located on the territory of the Company and in data centers on the territory of the Russian Federation.
	6. The Company does not carry out cross-border transfer of personal data.
	7. The Company does not make decisions that generate legal consequences in relation to personal data subjects or otherwise affect their rights and legitimate interests based solely on automated processing of personal data. Data that has legal consequences or affects the rights and legitimate interests of the Employee, such as the amount of accrued income, taxes and other deductions, are subject to verification by an authorized employee of the Company before their use.

# Methods of processing personal data

* 1. The Company processes personal data using automation tools, as well as without using such tools.
	2. The Policy applies in full to the processing of personal data using automation tools, and when processing personal data without the use of automation tools, to those cases where such processing corresponds to the nature of the actions (operations) performed with personal data using automation tools, i.e. allows for the search for personal data recorded on a tangible medium and contained in card indexes or other systematized collections of personal data, and (or) access to such personal data, in accordance with a specified algorithm.

# Confidentiality of personal data

* 1. Employees of the Company who have received access to personal data must ensure the confidentiality of such data, with the exception of information for which the subjects have given consent for their dissemination.
	2. The Company has the right, with the consent of the subject, to assign the processing of personal data to another person, unless otherwise provided by law, on the basis of an agreement concluded with this person, which provides as an essential condition the obligation of the person processing personal data on behalf of the Company to comply with the principles and rules for processing personal data provided by law. The volume of personal data transferred to another person for processing, the actions performed with personal data by this person must be the minimum necessary for the fulfillment of their obligations to the Company.

The Company's order must define the list of actions (operations) with personal data that will be performed by the person processing the personal data, the purposes of processing, the list of personal data processed under the order, the obligation of such person to maintain the confidentiality of personal data and ensure the security of personal data during their processing, at the request of the Company during the term of the order, including before the processing of personal data, to provide documents and other information confirming the adoption of measures and compliance with the requirements established by Article 6 of Federal Law No. 152-FZ of 27.07.2006 "On Personal Data" for the purpose of executing the operator's order, to notify the operator of facts of unlawful or accidental transfer (provision, distribution, access) of personal data that has resulted in a violation of the rights of personal data subjects, as well as the requirements for the protection of personal data being processed in accordance with Article 19 of the said law.

When executing the Company's order to process personal data, the person to whom such processing is entrusted has the right to use their information systems for processing personal data that comply with the security requirements established by law, which is reflected by the Company in the concluded agreement on the order to process personal data.

* 1. If the Company entrusts the processing of personal data to another person, the Company shall be liable to the subject of personal data for the actions of the said person. The person processing personal data on behalf of the Company shall be liable to the Company.

If the Company entrusts the processing of personal data to a foreign individual or foreign legal entity, the Company and the person processing the personal data on behalf of the Company shall be liable to the subject of the personal data for the actions of the said persons.

* 1. The Company has the right to place its personal data information systems in a data center (cloud computing infrastructure). In this case, the agreement with the data center (cloud service provider) includes as a material condition a requirement to prohibit access of the data center personnel to the Company's personal data information systems placed in the data center (cloud infrastructure), and this placement is not considered by the Company as an assignment of personal data processing to the data center (cloud service provider) and does not require the consent of the personal data subjects to such placement.

# Consent of the subject of personal data to the processing of their personal data

* 1. The subject of personal data makes a decision to provide their personal data to the Company and gives consent to their processing freely, of their own free will and in their interests. Consent to the processing of personal data must be specific, objective, informed, conscious and unambiguous and may be provided by the subject in any form that allows confirmation of the fact of its receipt, unless otherwise established by law.
	2. In the event that the Company receives personal data from a counterparty on the basis of and for the purpose of concluding and/or executing an agreement concluded with it, including from other companies of the group, responsibility for the legality and accuracy of the personal data, as well as for obtaining the consent of the Representatives of the counterpartiesand the responsibility for the transfer of personal data of the Employees of the group of companies to the Company lies with the counterparty transferring the personal data, which is stipulated in the text of the agreement with the counterparty.
	3. The Company that has received personal data from the counterparty does not undertake the obligation to inform the subjects (their representatives) whose personal data have been transferred to it about the commencement of the processing of personal data, since the obligation to provide the relevant information when concluding an agreement with the subject of personal data and/or when receiving consent for such transfer is borne by the counterparty that transferred the personal data. This obligation of the counterparty is included in the agreement concluded with it by the Company.
	4. The express consent of the Employee for the processing of his personal data is not required, since the processing is necessary for the performance of the employment contract to which the Employee, the subject of personal data, is a party, except for cases where it is necessary to obtain the Employee's consent in writing for specific cases of personal data processing. Cases requiring the Employee's consent in writing include (without limitation):
		1. Obtaining personal data of Employees from third parties, including for the purpose of verifying such personal data, as well as in cases where such data cannot be obtained from the Employee himself.
		2. Transfer of the Employee's personal data to any third party, including the transfer of the Employee's personal data when sending them on business trips, for training and advanced training, when booking hotels and tickets, etc.
		3. Transfer of the Employee's personal data to third parties for commercial purposes, including banks that open and service payment cards for calculating the Employee's salary and other income, insurance companies and/or medical organizations when concluding and executing insurance contracts for Employees at the expense of the Company as an employer, printing companies engaged in the production of business cards (business cards) for Employees at the expense of the employer, organizers of business exhibitions and conferences, organizations engaged in providing business trips, booking tickets, etc.
		4. Transfer of the Employee's personal data to organizations providing consulting services and comprehensive support for the Company's activities in the field of accounting, tax and personnel records, labor protection, material and technical support and other support for the Company's activities.
		5. Transfer of the Employee's personal data to notaries for the execution of notarized powers of attorney on behalf of the Company and the performance of other notarial actions.
		6. Transfer of personal data of the Employee organizations providing services and performing work on the implementation of software products and databases intended for the automation of management and accounting for the purpose of implementing software products and databases intended for the automation of management and accounting in the Company into the activities of the Company.
		7. Transfer of personal data of the Employee to charitable foundations for the purpose of transferring voluntary donations from Employees.
		8. Transfer of the Employee's personal data to contractors providing housing for rent to employees, as well as cars for rent to employees.
		9. Transfer of the Employee's personal data to tax counterparties for the purpose of consulting on tax issues.
		10. Transfer of personal data of the Employee contractors providing educational services.
		11. Transfer of personal data of the Employee to outsourcing companies that provide visas for foreign countries when sending the Company's Employees on foreign business trips, visa support, obtaining work permits and migration registration of employees who are not citizens of the Russian Federation.
		12. Transfer of personal data to the landlord for the purpose of ensuring access of Employees to secure rented premises.
	5. The express consent of the Family Members of the Company's employees is not required if the processing of their personal data is carried out on the basis of legislation (for the calculation of alimony, registration of social payments, provision of benefits and guarantees, etc.), is performed by the Company as an employer in accordance with the requirements of the Labor Code of the Russian Federation and state statistical authorities, as well as in cases where the Family Members of the employees are beneficiaries, including insured persons under contracts concluded by the Company as an insurer in favor of the Family Members of the employees, recipients of educational and consulting services. In all other cases, it is necessary to obtain demonstrable (confirmable) consent of the Family Members of the employees for the processing of their personal data by the Company.
	6. The express consent of the Applicants for the processing of their personal data is not required, since such processing is necessary for the purpose of concluding employment contracts at the initiative of the Applicants - subjects of personal data, except for cases when it is necessary to obtain the consent of the Applicant in writing for specific cases of personal data processing. The personal data of the Applicant contained in his/her questionnaire, resume, e-mails sent to the Company by the Applicant or specialized personnel selection organizations, and other documents, are processed in the manner prescribed by the current legislation of the Russian Federation.

In other cases, including when the Company approaches the Applicant with a job offer, in order to process the Applicant’s personal data, it is necessary to obtain his consent to the processing of personal data in any provable form, for example, in the text of the questionnaire, by e-mail, etc.

* 1. The consent of the Participants of the case championships is given in any provable form, for example, by obtaining consent in paper form when participating in person offline, or by sending a scanned copy (photo) of the Consent by e-mail, etc.
	2. The consent of the Participants of career events is given in any provable form, for example, by obtaining consent in paper form when participating in person offline, or by sending a scanned copy (photograph) of the Consent by e-mail, etc.;
	3. The consent of Consumers is provided in the form of implicative actions by providing their personal data in documents transferred to the Company and accepting the terms of the relevant events, competitions, user agreements, as well as by placing marks when filling out the relevant forms on the Company's websites.
	4. Personal data of persons who have signed contracts with the Company and contained in the unified state registers of legal entities and individual entrepreneurs are open and publicly available, with the exception of information about the number, date of issue and the authority that issued the identity document of an individual. Protection of their confidentiality and the consent of personal data subjects to the processing of such data is not required.

In all other cases, it is necessary to obtain the consent of the personal data subjects who are the Representatives of the counterparties, with the exception of persons who have signed agreements with the Company, provided powers of attorney to act on behalf of and on behalf of the Company's counterparties and thereby performed implicative actions confirming their consent to the processing of personal data specified in the text of the agreement (power of attorney). The consent of the Representative of the counterparty to the transfer of his personal data to the Company and the processing of such data by him may be obtained by the counterparty in the manner described in paragraph 7.2 of the Policy. In this case, the Company does not need to obtain the consent of the subject to the processing of his personal data.

* 1. The consent of the Representatives of personal data subjects to the processing of their personal data is expressed in the form of implicit actions by providing a power of attorney with the right to act on behalf of and on behalf of the personal data subjects and a document certifying the identity of the Representative of the personal data subject.
	2. The Visitor’s consent to the processing of his personal data is given in the form of implicit actions, namely, the provision of an identity document and the communication of information requested from him when visiting the Company.
	3. The consent of the Users of the websites to the processing of their personal data received by the Company when Visitors view the pages of the Company's websites on the Internet is given by accepting the terms of the "Cookie Policy " and placing the appropriate mark ("checkbox") in the banners on the Company's websites.
	4. If it is necessary to obtain the consent of the subject to the processing of personal data in written form, such consent may be obtained in the form of an electronic document signed with an electronic signature in accordance with the requirements established by law.
	5. The consent of subjects to the provision of their personal data is not required when the Company receives, within the framework of its established powers, reasoned requests from prosecutorial authorities, law enforcement agencies, investigative and inquiry agencies, security agencies, from state labor inspectors when they exercise state supervision and control over compliance with labor legislation, and other bodies authorized to request information in accordance with the competence provided for by law.

A reasoned request must include an indication of the purpose of the request, a reference to the legal basis for the request, including confirmation of the authority of the body that sent the request, and a list of the requested information.

* 1. In the event of requests from organizations that do not have the appropriate authority, the Company is obliged to obtain consent from the subject to provide their personal data and to warn the persons receiving the personal data that this data may only be used for the purposes for which it was communicated, and also to require these persons to confirm that the specified rule will (has) been observed. The procedure for obtaining consent from Employees to transfer their personal data to other persons is described in paragraph 7.4 of the Policy.
	2. In all cases, the obligation to provide proof of obtaining the consent of the personal data subject to the processing of his personal data or proof of the existence of the grounds specified in the Federal Law of 27.07.2006 No. 152-FZ "On Personal Data" is assigned to the Company.

# Rights of personal data subjects

* 1. The subject of personal data has the right to receive information concerning the processing of his personal data, including information containing:
* confirmation of the fact that his personal data is being processed by the Company;
* legal grounds and purposes of processing personal data;
* information on the methods of processing personal data used by the Company;
* the name and location of the Company, information about persons (except for employees of the Company) who have access to personal data or to whom personal data may be disclosed on the basis of an agreement with the Company or on the basis of legislation;
* processed personal data relating to the relevant personal data subject, the source of their receipt;
* terms of processing personal data, including the terms of their storage;
* the procedure for the exercise by the subject of personal data of the rights provided for by the Federal Law of 27.07.2006 No. 152-FZ "On Personal Data";
* information on the completed or intended cross-border transfer of data;
* the name or surname, first name, patronymic and address of the person processing personal data on behalf of the operator, if the processing is or will be entrusted to such person;
* information on the methods of fulfilling by the Company as an operator the obligations established by Article 18.1 of the Federal Law of 27.07.2006 No. 152-FZ “On Personal Data”;
* other information provided by law.

The specified information must be provided to the subject of personal data by an authorized employee of the Company in an accessible form, and it must not contain personal data related to other subjects of personal data, except in cases where there are legal grounds for disclosing such personal data (for example, information on the processing of personal data of family members of employees).

* 1. If the personal data subject believes that the Company processes his personal data in violation of the requirements of the law or otherwise violates his rights and freedoms, the personal data subject has the right to appeal the actions or inaction of the Company to the authorized body for the protection of the rights of personal data subjects (Roskomnadzor) or in court.
	2. The subject of personal data has the right to protect his rights and legitimate interests, including compensation for losses and (or) compensation for moral damages in court.

# Information on the implemented requirements for the protection of personal data

* 1. The security of personal data processed by the Company is ensured by the implementation of legal, organizational and technical measures necessary and sufficient to meet the requirements of the legislation on personal data.
	2. Legal measures taken by the Society include:
* development of local acts of the Company implementing the requirements of the legislation, including the Policy and Regulation on the procedure for processing and ensuring the security of
personal data in the Company;
* refusal of any methods of processing personal data that do not correspond to the purposes specified in the Policy and the requirements of the law.
	1. Organizational measures taken by the Society include:
* appointment of a person responsible for organizing the processing of personal data;
* appointment of a person responsible for ensuring the security of personal data in personal data information systems;
* limiting the number of employees of the Company who have access to personal data and organizing a permit system for access to them;
* familiarization of the Company's employees directly involved in the processing of personal data with the provisions of the legislation on personal data, including the requirements for the protection of personal data, with the Policy, and other local acts of the Company on issues of processing personal data;
* training of all categories of the Company’s employees directly involved in the processing of personal data in the rules for working with them and ensuring the security of the data being processed;
* defining in the job descriptions of the Company’s employees the responsibilities for ensuring the security of personal data processing and liability for violation of the established procedure;
* regulation of personal data processing processes;
* organization of accounting of material carriers of personal data and their storage, ensuring the prevention of theft, substitution, unauthorized copying and destruction;
* determination of the type of threats to the security of personal data relevant to personal data information systems, taking into account the assessment of the possible harm to personal data subjects that may be caused in the event of a violation of security requirements, determination of the level of protection of personal data and requirements for the protection of personal data when processing them in information systems, the implementation of which ensures the established levels of protection of personal data;
* identification of threats to the security of personal data when processing them in information systems, and the formation of a private model (models) of current threats on their basis;
* placement of technical means for processing personal data within the protected area;
* restricting access of unauthorized persons to the Company's premises, preventing them from being in premises where work is carried out with personal data and technical means of processing them are located, without supervision by the Company's employees.
	1. Technical measures taken by the Company include:
* development, based on a private model of current threats, of a system for protecting personal data for the levels of protection of personal data established by the Government of the Russian Federation when processing them in information systems;
* use of information security tools that have undergone a compliance assessment procedure to neutralize current threats;
* assessment of the effectiveness of measures taken to ensure the security of personal data;
* implementation of a permit system for employee access to personal data processed in information systems and to hardware and software for information protection;
* registration and accounting of actions with personal data of users of information systems where personal data is processed;
* software environment limitation;
* detection of malicious software (use of antivirus programs) on all nodes of the Company’s information network that provide the appropriate technical capability;
* secure internetworking (use of firewalls);
* identification and authentication of the user when logging into the information system using a password;
* control of software integrity, including information security software;
* detection of intrusions into the Company’s information system that violate or create preconditions for the violation of established requirements for ensuring the security of personal data;
* protection of the virtualization environment;
* protection of network devices and communication channels through which personal data is transmitted;
* restoration of personal data modified or destroyed due to unauthorized access to them (creation of a system for backup and restoration of personal data);
* monitoring compliance with these requirements (independently or with the involvement, on a contractual basis, of legal entities and individual entrepreneurs licensed to carry out activities for the technical protection of confidential information) at least once every 3 years.

# Final Provisions

* 1. Other obligations and rights of the Company as an operator of personal data and a person organizing their processing on behalf of other operators are determined by legislation in the field of personal data.
	2. Officials and Employees of the Company guilty of violating the rules governing the processing and protection of personal data shall bear material, disciplinary, administrative, civil and criminal liability in accordance with the law.
	3. The Policy is revised as necessary. Mandatory revision of the Policy is carried out in the event of significant changes in international or legislation in the field of personal data.

When making changes to the Policy, the following is taken into account:

* changes in the information infrastructure and/or in the information technologies used by the Company;
* the established practice in the Russian Federation of law enforcement of legislation in the field of personal data;
* changes in the conditions and features of processing personal data by the Company in connection with the introduction of new information systems, processes and technologies into its activities.