Limited Liability Company «KOMNET» (Rightech)

(full operator name)

"APPROVED"

Director General — (title)

Bikonya Iliya Vladimirovich — (signature) (print full name)

№ 2019/08-01

26th of August 2019

Internal rules for data protection

1. General Terms

1.1. This Regulation has been developed in accordance with the current laws of the Russian Federation Concerning Personal Data (hereinafter referred to as Personal Data) and regulatory and methodological documents of the executive bodies of state power on the security of Personal Data when processing them in Information Systems of Personal Data (hereinafter referred to as ISPD).

1.2. For the purposes of this Regulation, the following terms shall be used:

personal data (PD) - any information relating directly or indirectly to a specific or determined individual (subject of Personal Data);

operator - a legal entity that organizes and/or carries out Personal Data processing independently or jointly with other persons, as well as determining the purpose of Personal Data processing; the composition of Personal Data to be processed, actions (operations) performed with Personal Data;

PD processing - any action (operation) or a set of actions (operations) performed using automation means or without using such means with PD, including collection, recording, systematization, accumulation, storage, refinement (updating, modification), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, removal, destruction of PD;

automated PD processing - PD processing using computer equipment;

distribution of PD - actions aimed at revealing PD to an indefinite circle of persons;

Provision of PD - actions aimed at disclosing PD to a certain person or a certain circle of persons;

PD blocking - temporary termination of PD processing (except if processing is necessary to clarify PD);

destruction of PD - actions that make it impossible to restore the Personal Data content in Personal Data systems and/or as a result of which material carriers of PD are destroyed;

depersonalization of PD - actions that make it impossible without the use of additional information to determine the belonging of PD to a particular subject of PD;

information system of personal data (ISPD) - set of the information technologies and technical means which are contained in the PD databases and providing their processing;

transboundary transfer of PD - transfer of PD to the territory of a foreign state to an authority of a foreign state, a foreign natural person or a foreign legal person.

1.3. This Regulation defines the procedure and conditions for processing Personal Data in the Limited Liability Company "KOMNET" (hereinafter referred to as the Operator), including the procedure for transferring Personal Data to third parties, features of automated and non-automated Personal Data processing, the procedure for access to Personal Data, the Personal Data protection system, the procedure for organizing internal control and liability for violations during processing

1.4. This Regulation applies to all processes for collection, systematization, accumulation, storage, clarification, use, distribution (including transfer), depersonalization, blocking, destruction of personal data carried out using automation means and without their use.

1.5. The present Regulation shall come into force from the date of its approval by the General Director of the Operator and shall remain in force indefinitely until being replaced by a new Regulation.

1.6. All amendments to the Regulation are made pursuant to the order.

1.7. All employees of the Operator shall be familiarized with this Regulation with written acknowledgement of receipt.

2. Scope and Objectives of Personal Data processing

2.1. The processing of Personal Data shall be limited to the achievement of specific, predetermined and legitimate purposes. Personal Data processing incompatible with the purposes of Personal Data collection is not allowed.

2.2. Databases containing Personal Data which are processed for purposes incompatible with each other shall not be merged.

2.3. Only Personal Data that meet the purposes of their processing shall be processed.

2.4. The content and scope of the Personal Data processed shall be in accordance with the stated purposes of the processing. The Personal Data processed shall not be redundant with respect to the stated purposes of their processing.

2.5. Processing of Personal Data of the Operator's Employees may be carried out solely in order to ensure compliance with laws and other regulatory legal acts, to assist employees in employment, training and promotion on the career ladder, to ensure personal safety of employees, to control the quantity and quality of work performed and to ensure the safety of the Operator's property.

2.6. The main objectives of Personal Data processing are: conclusion, execution and termination of labor and civil law agreements with employees, citizens, legal entities, individual entrepreneurs and other persons in situations provided for by law and the Charter; Personnel records management; compliance with the requirements of tax legislation, pension legislation in the formation and transfer to the Pension Fund of the Russian Federation of personalized data on each recipient of income, which are taken into account when accruing contributions to compulsory pension insurance, filling in primary statistical documentation in accordance with the Labor, Tax Code and federal laws.

2.7. ISPD provides the following tasks: personnel accounting, accounting and control over financial and economic activities, fulfillment of financial obligations under concluded contracts, ensuring personal security of employees and other tasks.

3. Personal Data processed by IDPS

3.1. The following PD subjects are processed in ISPD:

3.2. operator's employees;

3.3. candidates for employment;

3.4. shareholders/founders of the Operator, persons associated with employees, shareholders, founders (children in respect of whom alimony is paid, wives, etc.);

3.5. customers (users of the Operator's services);

3.6. individual entrepreneurs - counterparties of the Operator;

3.7. clients of organizations, counterparties of the Operator (servicing corporate clients);

3.8. Other natural persons whose personal data are processed by the Operator.

3.9. This list may be revised as necessary.

3.10. Personal data of PD subjects include:

- last name, first name, patronymic;
- date of birth;
- citizenship;
- number of insurance certificate;
- TIN;
- Knowledge of foreign languages;
- data on education (number, series of diplomas, year of graduation);
- data on acquired specialties;
- marital status;
- actual place of residence;
- contact information;
- data on military duty;
- data on current employment (date of employment start, personnel movements, salaries and their changes, information on incentives, data on professional development, etc.).

3.11. Complete lists of processed PD are generated in the list of PD to be protected in the Operator's ISPD.

4. Access to Personal Data

4.1. The Operator's employees who, by virtue of their official duties, constantly work with the Personal Data, shall be admitted to the necessary categories of Personal Data for the duration of their respective official duties on the basis of the list of persons admitted to work with the Personal Data, which is approved by the Operator's Manager.

4.2. The list of persons having access to the Personal Data for the information system should be kept up to date.

4.3. The operator has established a permitting procedure for access to Personal Data. The Operator's employees shall have access to work with Personal Data only within the limits and scope necessary for the performance of their duties on the basis of the decision of the Manager

4.4. Temporary or one-time admission to work with Personal Data due to business necessity may be obtained by the Operator's employee upon agreement of the Manager.

4.5. Access to Personal Data of third parties who are not employees of the Operator without the consent of the personal data subject is prohibited, with the exception of access of employees of executive authorities carried out as part of measures to monitor and supervise the implementation of legislation, the implementation of functions and powers of relevant state authorities. The information shall be provided upon request or request of the state authority with the knowledge of the Operator's Head.

4.6. In case an employee of a third-party organization needs access to the Operator's Personal Data, it is necessary that the Contract with the third-party organization sets out the terms of confidentiality of the personal data and the obligation of the third-party organization and its employees to comply with the requirements of the current legislation in the field of personal data protection. In addition, in case of access to personal data of persons who are not employees of the Operator, consent of the personal data subjects to provide their personal data to third parties shall be obtained. This consent is not required if the IDs are provided for the purpose of execution of the civil contract concluded by the Operator with the subject of Personal Data.

4.7. Access of the Operator's employee to the personal data shall be terminated from the date of termination of the employment relationship or the date of change of the employee's job responsibilities and/or removal of the employee from

the list of persons entitled to access the personal data. In case of dismissal, all media containing Personal Data, which in accordance with the job duties were at the disposal of the employee during work, must be transferred to the appropriate official.

5. Principal requirements for Personal Data protection

5.1. During PD processing in the information system, the following shall be ensured:

a) carrying out measures aimed at preventing unauthorized access to personal data and/or their transfer to persons who do not have the right to access such information;

b) timely detection of unauthorized access to personal data;

c) prevention of impact on technical means of automatic processing of personal data, as a result of which their functioning can be disrupted;

d) possibility of immediate restoration of PD, modified or destroyed due to unauthorized access to them;

e) constant control over ensuring the level of Personal Data protection.

5.2. The operator is obliged to take the necessary legal, organizational, technical and other measures to ensure the safety of personal data.

5.3. The operator shall use equipment and software for PD processing and protection.

5.4. Employees shall immediately inform the relevant official of the Operator about the loss or lack of information carriers that make up the Personal Data sheet, as well as about the causes and conditions of possible leakage of Personal Data sheet. In the event of an attempt by unauthorized persons to obtain PD from an employee processed by the Operator, an immediate notification shall be made to the relevant official of the Operator.

6. Consent to Personal Data processing

6.1. The subject of PD decides to grant its PD and agrees to process it freely and by its will and in its interest. Consent to processing PD must be specific, informed and conscious. Consent to the processing of PD may be given by the personal data subject or his representative in any form that allows to confirm the fact of its receipt, unless otherwise established by the legislation of the Russian Federation. In case of obtaining consent for processing of PD from the representative of the PD subject, the authority of this representative to give consent on behalf of the personal data subject shall be checked by the Operator.

6.2. Receipt of written consent for personal data processing shall be carried out by the Operator's employee, upon receipt of personal data from the personal data subject, by making written consent according to the form established by the Operator.

7. Rights of the subject in relation to PD processed by the Operator

7.1. The subject of PD has the right to:

- to receive information from the Operator concerning processing of its PD. The information shall be provided to the subject of the PD by the Operator in accessible form and shall not contain PD relating to other PD entities, unless there are legitimate grounds for disclosing such PD. The list of information and the procedure for obtaining information is provided by the current legislation of the Russian Federation;
- require the Operator to clarify its personal data, block or destroy them if the personal data are incomplete, obsolete, inaccurate, illegally obtained or are not necessary for the stated purpose of processing, as well as take measures provided by the legislation of the Russian Federation to protect their rights;
- to the condition of prior written consent when processing personal data for the purpose of promotion of goods, works, services in the market by making direct contacts with a potential consumer by means of communication, as well as for the purpose of political agitation;

- on the condition of written consent when making decisions of the Operator on the basis of exclusively automated processing of personal data, which give rise to legal consequences in relation to the subject of personal data or otherwise affecting its rights and legitimate interests;
- object to the decisions of the Operator based solely on automated processing of its PD and possible legal consequences of such decision;
- to appeal the Operator's actions or omissions to the authorized body for protection of the rights of PD subjects or in court.

8. Rights and Obligations of the ISPD Operator

8.1.1. The ISPD Operator may:

8.1.2. To entrust the processing of PD to another person with the consent of the subject of the PD, unless otherwise provided by federal law, on the basis of an agreement concluded with this person, including a state or municipal contract, or by adopting an appropriate act by a state or municipal body.

8.1.3. If the subject of the PD withdraws consent to processing PD, continues processing PD without the consent of the subject of the PD if there are grounds specified in the legislation of the Russian Federation.

8.1.4. Refuse to the subject of the PD to perform a repeated request for information that does not meet the conditions stipulated by the legislation of the Russian Federation. Such a refusal must be motivated. It is the responsibility of the operator to provide proof of the validity of the refusal to execute the repeated request.

8.1.5. Independently determine the composition and list of measures necessary and sufficient to ensure the fulfillment of the duties of the HIPC Operator stipulated by the legislation of the Russian Federation.

8.1.6. The ISPD operator shall:

8.1.7. The operator is obliged to notify the authorized body for protection of the rights of the PD subjects about his intention to process personal data before the start of processing of PD, except in cases stipulated by the legislation of the Russian Federation.

8.1.8. When gaining access to PD, not disclose or distribute PD to third parties without the consent of the personal data subject, unless otherwise provided by federal law.

8.1.9. Provide proof of obtaining the consent of the PD subject to the processing of his PD or proof of the existence of legal grounds, processing of PD without the consent of the PD subject.

8.1.10. Prior to the commencement of the cross-border transfer of PD, to ensure that the rights of the PD subjects are adequately protected by the foreign State to which territory the PD is transferred.

8.1.11. At the request of the PD subject, in order to promote goods, works, services in the market by making direct contacts with a potential consumer through communication means, as well as for the purpose of political agitation - to stop processing its PD.

8.1.12. Explain to the PD subject the procedure for making a decision based solely on the automated processing of its PD and the possible legal consequences of such a decision, provide an opportunity to object to such a decision, as well as explain the procedure for protecting the PD subject's rights and legitimate interests.

The Operator shall consider the objection within thirty days from the date of its receipt and notify the subject of PD of the results of the consideration of such an objection.

8.1.13. When collecting PD, provide the subject of PD at his request with the information provided by the legislation of the Russian Federation.

8.1.14. If the provision of PD to the Operator for the PD subject is mandatory in accordance with federal law, the Operator shall explain to the PD subject the legal consequences of the refusal to provide its PD.

8.1.15. If the PD is not received from the subject of PD, the Operator shall, except as provided by the legislation of the Russian Federation, provide the subject of PD with the following information prior to processing such PD:

1) name or surname, first name, patronymic and address of the operator or his representative;

2) purpose of PD processing and its legal basis;

3) prospective PD users;

4) the rights of the subject of PD established by this Federal Law;

5) a source of PD production.

8.1.16. To take measures necessary and sufficient to ensure the fulfillment of the duties of the ISPD Operator provided by the legislation of the Russian Federation.

8.1.17. Publish or otherwise provide unrestricted access to the document defining its PD processing policy to information about the applicable PD protection requirements.

8.1.18. When collecting personal data using information and telecommunication networks, publish in the corresponding information and telecommunication network a document defining its policy regarding the processing of personal data, and information on the implemented requirements for the protection of personal data, as well as provide access to the specified document using the funds of the corresponding information and telecommunication network.

8.1.19. To submit documents and local acts stipulated by the legislation of the Russian Federation and/or otherwise confirm the adoption of measures necessary and sufficient to ensure the fulfillment of the duties of the ISPD Operator, at the request of the authorized body for the protection of the rights of ISPD subjects.

8.1.20. When processing personal data, take the necessary legal, organizational and technical measures or ensure that they are taken to protect personal data against unlawful or accidental access to them, destruction, modification, blocking, copying, provision, distribution of personal data, as well as against other unlawful actions in relation to personal data.

8.1.21. Inform the PD subject or its representative free of charge of the availability of PD related to the relevant PD subject in the manner provided by the legislation of the Russian Federation, and also provide an opportunity to familiarize themselves with these PD when the PD subject or his representative applies or within thirty days from the date of receiving the request of the subject of PD or his representative.

8.1.22. In case of refusal to provide information on the presence of PD about the relevant PD subject or PD subject to the PD subject or its representative upon their request or upon receipt of the request of the PD subject or its representative, the operator shall give a motivated response in writing, containing a reference to a provision of the legislation of the Russian Federation that is the basis for such a refusal, within thirty days from the date of application of the PD subject or its representative or from the date of receipt of the request of the PD subject or its representative.

8.1.23. Within a term not exceeding seven working days from the date of submission by the PD subject or his representative of information confirming that personal data are incomplete, inaccurate or irrelevant, the Operator shall make the necessary changes to them. Within a term not exceeding seven working days from the date of submission by the PD subject or his representative of information confirming that such personal data are illegally obtained or are not necessary for the stated purpose of processing, the operator is obliged to destroy such personal data. The operator shall notify the PD subject or its representative of the changes made to and measures taken of and take reasonable steps to notify third parties to whom PD of that subject has been transferred.

8.1.24. To inform the authorized body for protection of the rights of PD subjects at the request of this body the necessary information within thirty days from the date of receipt of such a request.

8.1.25. In case of detection of improper processing of PD performed by the Operator or a person acting on behalf of the Operator, the Operator shall, within a term not exceeding three working days from the date of this detection, cease improper processing of PD or ensure termination of improper processing of PD by a person acting on behalf of the Operator. In the event that it is impossible to ensure the lawfulness of PD processing, the Operator shall, within a term not exceeding ten working days from the date of detection of improper PD processing, destroy such PD or ensure its destruction. The Operator shall notify the PD subject or its representative about the elimination of the violations or about the destruction of the PD, and in case the appeal of the PD subject or its representative or make a request of the authorized body for protection of the PD subjects rights was sent by the authorized body for protection of the PD subject rights, also the specified body.

8.1.26. If the purpose of PD processing is achieved, the Operator shall terminate PD processing or ensure its termination (if the PD is processed by another person acting on behalf of the Operator) and destroy the PD or ensure their destruction (if the PD is processed by another person acting on behalf of the Operator) on time, not exceeding thirty days from the date of achievement of the PD processing objective, unless otherwise provided by a Contract to which the beneficiary or guarantor is a party, according to which is the personal data subject, another agreement between the Operator and the personal data subject, or if the Operator is not entitled to perform personal data processing without the consent of the personal data subject on the grounds stipulated by the legislation of the Russian Federation.

8.1.27. In case of revocation by the PD subject of consent to processing its PD - to stop its processing or ensure termination of such processing (if the PD is processed by another person acting on behalf of the Operator) and if the PD is no longer required for the purpose of PD processing - destroy the PD or ensure its destruction (if the PD is processed by another person acting on behalf of the Operator) on time, not exceeding thirty days from the date of receipt of said withdrawal, unless otherwise provided by the Contract, a party to which the beneficiary or guarantor is a PD subject, other agreement between the operator and the PD subject or if the Operator is not entitled to process PD without the consent of the PD subject on the grounds stipulated by the legislation of the Russian Federation.

8.1.28. Assign a person responsible for organizing the PD processing.

9. Processing and Protection procedure of Personal Data

9.1.1. Ensuring confidentiality of personal data processed by the Operator is a mandatory requirement for all persons to whom personal data are known.

9.1.2. The Operator's employees who execute the documents are obliged to obtain the consent of the personal data subjects for processing in established cases.

9.1.3. In case of violation of the established procedure for processing personal data, the Operator's employees shall be liable in accordance with Section 9 of this Regulation.

9.1.4. Personal data of paper-based entities processed by the Operator are stored in departments (with employees) that have permission to process the corresponding personal data. The right to admit employees to non-automated ISPD is determined by the order of the Head. PD carriers shall not be left unattended. When leaving the workplace, personnel handling personal data shall remove the media in a safe, lockable cabinet or otherwise restrict unauthorized access to the media. In case of loss or damage of PD, their restoration is carried out if possible.

9.1.5. 9.5. Storage places of documents containing PD:

9.1.6. 9.5.1. Personal data of the Operator's clients (contracts, acts, agreements, questionnaires, copies of passports, other similar documents containing personal data of the Operator's customers, information carriers (flash cards, CDs, etc.) are stored in the main and spare offices of the Operator, placed on shelves and locked to the key. The responsible person exercising control shall be determined by the order of the Manager.

9.1.7. Personal data of the Operator's employees - documents, information carriers (flash cards, CDs, etc.) are stored in the company's safe and locked to the key. The responsible person exercising control is the Operator's Manager.

9.1.8. The issuance of documents for familiarization is carried out by persons admitted to the relevant information for the purpose of performing official duties for a period of not more than one working day.

9.1.9. Other media may be stored in the main and spare offices of the Operator, placed on shelves and locked to the key or in the safe of the organization. The responsible person exercising control over other information carriers shall be determined by the order of the Head.

9.1.10. When working with software tools of the Operator's automated system, which implements the functions of viewing and editing personal data, it is prohibited to demonstrate screen forms containing such data to persons who do not have the appropriate permission.

9.1.11. Upon receipt of the Personal Data by the Operator's employee, who in accordance with his official duties receives the Personal Data from the client, the employee of another person is required to verify the validity of the Personal Data. Entry of personal data received by the Operator into the information system is carried out by employees with access to the

corresponding personal data. Employees who enter information are responsible for the reliability and completeness of the entered information.

9.1.12. The peculiarities of processing personal data contained on paper media without the use of automation tools (PC is not used when compiling documents) are established in accordance with the Decree of the Government of the Russian Federation of 15.09.2008 N 687 "On approval of the Regulation on the peculiarities of personal data processing carried out without the use of automation tools."

9.1.13. In non-automated processing of different PD categories, a separate material carrier shall be used for each PD category.

9.1.14. In case of non-automated processing of personal data on paper:

9.1.15. It is not allowed to fix personal data on one paper medium, the purposes of processing of which are obviously incompatible;

9.1.16. Personal data should be separated from other information, in particular by fixing it on separate paper media, in special sections or in the fields of forms (forms);

9.1.17. When using standard forms of documents in which the nature of the information implies or allows the inclusion of personal data (hereinafter referred to as standard forms), the following conditions shall be met:

9.1.18. The standard form or related documents (instructions for its completion, cards, registers and journals) shall contain information about the purpose of non-automated processing of personal data, name (name) and address of the Operator, surname, first name, patronymic and address of the PD subject, source of receipt of personal data, terms of processing of personal data, list of actions with personal data to be performed during their processing, general

9.1.19. The template should provide for a field in which the PD subject can indicate his or her consent to non-automated PD processing - if it is necessary to obtain written consent to the PD processing;

9.1.20. The template should be designed in such a way that each of the PD subjects contained in the document has the opportunity to familiarize themselves with their PD contained in the document, without violating the rights and legitimate interests of other PD subjects;

9.1.21. The standard form should exclude the merging of fields intended for the introduction of PD, the purposes of which are obviously incompatible.

9.1.22. Storage of personal data shall be carried out in a form that allows determining the subject of personal data, no longer than the purpose of processing personal data, if the term of storage of personal data is not established by federal law, by a contract to which the beneficiary or guarantor under which the personal data subject is a party.

9.2. Cases of destruction, blocking and refinement of PD:

9.3. Destruction or depersonalization of part of personal data, if allowed by the material carrier, may be carried out in a way that excludes further processing of these personal data while preserving the possibility of processing other data recorded on the material carrier (removal, expurgation).

9.4. Refinement of personal data during their processing without the use of automation means is carried out by updating or changing data on the material medium, and if this is not allowed by the technical features of the material medium, by fixing on the same material medium information about changes made to them or by manufacturing a new material medium with updated personal data.

9.5. Destruction of carriers containing PD is carried out in the following order:

9.6. PD on paper media shall be destroyed by means of shredders (document destroyers) installed in the Operator's office.

9.7. PD placed in the PC memory are destroyed by removing it from the PC memory.

9.8. PD located on a flash card, CD, or other storage medium are destroyed by removing a file from the storage medium, if necessary by disrupting the flash card or CD.

9.9. The office, premises of the Operator, at the end of the working day and absence of employees in the office premises, shall be locked, the windows shall be closed, the alarm shall be activated (if any).

9.10. Network equipment, servers should be located in places inaccessible to unauthorized persons (in special rooms, cabinets, boxes).

9.11. Cleaning of premises and maintenance of ISPD equipment shall be carried out under the control of persons responsible for these premises and technical means with observance of measures excluding unauthorized access to ISPD, information carriers, software and technical means of processing, transmission and protection of ISPD information. It is the responsibility of ISPD administrators to manage ISPD user accounts, maintain the normal operation of ISPD, provide data backup, and install and configure ISPD hardware and software that is not related to ISPD security in ISPD. Also, it is the responsibility of the ISPD administrators to ensure that the procedure for processing and ensuring the security of ISPD where it meets the requirements for the confidentiality, integrity and accessibility of ISPD for a particular ISPD and the general safety requirements for PDPA established by federal law.

9.12. It is also the responsibility of ISPD administrators to install, configure and administer ISPD hardware and software security tools, record and store PD machine media, periodically audit security logs and analyze IDP security, as well as participate in official investigations of violations of the established procedure for processing and ensuring PD security.

9.13. In order to ensure the allocation of authority, mutual control and non-concentration critical to the security of the personal data, it is not recommended to combine the roles of the personal data system user and the personal data system administrator in the person of one employee.

9.14. Qualification requirements and a detailed list of the rights and obligations of ISPD administrators are enshrined in the relevant job descriptions, with which employees assigned to these roles must be familiarized with the signature.

9.15. Organization of internal control of the process of personal data processing by the Operator is carried out in order to study and evaluate the actual state of personal data protection, timely response to violations of the established procedure for their processing, as well as to improve this procedure and ensure its compliance.

9.16. Internal control measures for processing and ensuring the safety of personal data are aimed at solving the following tasks:

9.17. Ensuring that the Operator's employees comply with the requirements of this Regulation and regulations governing the scope of personal data.

9.18. Assessment of competence of personnel involved in PD processing. Ensuring the operability and efficiency of ISPD technical means and PD protection means, their compliance with the requirements of authorized executive authorities on the safety of PD.

9.19. Identification of violations of the established procedure for processing personal data and timely prevention of negative consequences of such violations.

9.20. Adoption of corrective measures aimed at elimination of detected violations, both in the procedure of PD processing and in the operation of ISPD equipment.

9.21. Development of recommendations to improve the procedure for processing and ensuring the safety of personal data based on the results of control measures

9.22. Internal monitoring of the implementation of recommendations and guidelines to address violations.

9.23. The results of control measures are drawn up by acts and are the basis for developing recommendations for improving the procedure for processing and ensuring the safety of personal data, for modernizing technical means of personal data and personal data protection, for training and improving the competence of personnel involved in personal data processing.

10. Operator Personal Data Management Features

10.1. This section sets out the additional rights and obligations of the Operator and employees in the processing of the Personal Data of the Operator's employees.

10.2. Employee's Personal Data - information required by the Operator in connection with the employment relationship and concerning the particular employee.

10.3. The processing of employee's personal data can be carried out solely for the purpose of ensuring compliance with laws and other regulatory legal acts, assisting employees in employment, training and promotion, ensuring the personal safety of employees, monitoring the quantity and quality of work performed and ensuring the safety of property.

10.4. The Operator shall not be entitled to receive and process the employee's personal data on his/her membership in public associations or his/her trade union activities, except as provided by federal laws;

10.5. In making decisions affecting the employee's interests, the Operator shall not be entitled to rely on the employee's personal data obtained solely as a result of their automated processing or electronic receipt;

10.6. Employees should not waive their rights to preserve and protect secrecy;

10.7. The Operator undertakes not to report the Personal Data to the Employee for commercial purposes without his written consent;

10.8. The Operator undertakes to warn the Operator's employees, third parties receiving the Employee's Personal Data (with their consent), that these data can be used only for the purposes for which they are reported and to require them to confirm that this rule is complied with. Persons receiving the employee's personal data are required to observe the secrecy (confidentiality) regime. The confidentiality regime shall be ensured by signing an agreement with a person (Annex to this Regulation). This provision does not apply to the exchange of personal data of employees in the manner established by the legislation of the Russian Federation;

10.9. Employees' personal data shall be accessed on the basis of orders and regulations approved by the Operator.

10.10. The Operator undertakes not to request information on the health status of the employee, except for that information related to the question of whether the employee can perform an employment function;

10.11. The Operator shall transfer the Employee's Personal Data to employee representatives in accordance with the procedure established by the legislation of the Russian Federation and limit this information only to those Employee's Personal Data required to perform their functions by the specified representatives.

10.12. A staff member has the right to identify his or her representatives to protect his or her personal data.

11. Liability for violation of this provision

11.1. The Operator's management shall be responsible for failure to ensure the confidentiality of the Personal Data and non-observance of the rights and freedoms of the Personal Data subjects in relation to their Personal Data, including the rights to privacy, personal and family secrets.

11.2. The Operator's employees bear personal responsibility for non-compliance with the requirements for processing and ensuring the safety of personal data set forth in this Regulation, in accordance with the legislation of the Russian Federation.

11.3. The Operator's employee may be held liable in the following cases:

11.4. Intentional or careless disclosure of PD

11.5. Loss of material carriers of personal data;

11.6. Violations of the requirements of this Regulation and other regulatory documents of the Operator regarding access and work with personal data

11.7. In cases of violation of the established procedure for processing and ensuring the safety of personal data, unauthorized access to personal data, disclosure of personal data and infliction of material or other damage to the Operator, its employees, customers and counterparties, the guilty persons shall bear civil, criminal, administrative, disciplinary and other liability stipulated by the legislation of the Russian Federation.