APPROVED by
Order of General Director of ITE Expo International LLC
No. 11-ОД dated 16 November 2022

Policy

for Processing and Security of Personal Data

of ITE Expo International LLC

Revision dated 16 November 2022

Moscow
2022

TABLE OF CONTENTS

1. General Provisions

1.1. This Policy (hereinafter referred to as the **"Policy"**) defines the general principles and procedure for personal data processing and measures to secure it of ITE Expo International LLC (hereinafter referred to as the **"Company"**).

The Policy objectives are to ensure that the rights and freedoms of a person and citizen are protected while their personal data is processed, including the rights to privacy, personal and family secrets, and that the requirements of the personal data laws and international personal data treaties of the Russian Federation are scrupulously and strictly complied with.

1.2. The Policy has been developed in accordance with the provisions of Federal Law On Personal Data No. 152-FZ dated 27 July 2006 and any other current regulatory legal acts that determine the procedure for handling personal data and the requirements for securing it (hereinafter referred to as the **"law"**) and subject to the Guidelines of the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) how to draw up a document defining the controller's policy for personal data processing in the manner prescribed by Federal Law On Personal Data No. 152-FZ dated 27 July 2006.

1.3. All employees of the Company must read, understand, and acknowledge by signing the Policy and any other by-laws of the Company that establish, in particular, the procedures aimed at preventing and identifying violations of the laws on processing and protecting personal data and at mitigating the effects thereof, as well as rights and obligations of the Company's employees in that area.

1.4. The following terms and definitions are used in the Policy:

automated personal data processing	means personal data processing by means of computer equipment
biometric personal data	means information that describes physiological and biological features of a person on the basis whereof their identity may be established and which is used by the controller to identify the personal data subject
personal data blocking	means suspension of personal data processing (except when such processing is required to clarify the personal data)
personal data access	means brining the personal data of subjects processed by the Company to the notice of certain persons (including the employees), provided that this information is kept confidential
personal data information system	means a set of personal data contained in databases and information technologies

	and technical facilities that enable its processing
confidentiality of personal data	means the obligation of persons who have gained access to the personal data not to disclose it to any third parties and not to disseminate the personal data without the consent of the personal data subject, unless otherwise provided for by law
personal data depersonalisation	means actions making it impossible to establish that the personal data belongs to a particular personal data subject without additional information
personal data processing	means any action (operation) or a set of actions (operations) with personal data that is carried out with or without using computer-aided facilities, including collecting, recording, systematising, accumulating, storing, clarifying (updating, modifying), retrieving, using, transferring (disseminating, sharing, access), depersonalising, blocking, deleting, destructing of personal data
controller	means a public authority, municipal authority, legal entity, or individual arranging and/or carrying out personal data processing, either independently or in cooperation with other parties and determining the processing purposes and scope of the personal data to be processed and actions (operations) with the personal data; In the Policy, the controller means the Company, unless otherwise specified.
personal data	means any information directly or indirectly related to an identified or identifiable individual (personal data subject)
personal data sharing	means actions aimed at disclosing the personal data to a certain person or a certain scope of persons
personal data dissemination	means actions aimed at disclosing the personal data to the general public
personal data subject	means an individual whom the personal data relates to

cross-border transfer of personal data	means transfer of the personal data to the territory of a foreign state to a government authority of a foreign state, a foreign individual or legal entity
personal data destruction	means actions rendering the personal data impossible to restore in the information system and/or resulting in the destruction of tangible media containing the personal data

2. Categories of Personal Data Subjects. Scope and Categories of Personal Data Processed by the Company

2.1. The Company is the personal data controller of the following categories of individuals:

Categories of Personal Data Subjects	Categories of Personal Data Processed by the Company
Applicants for vacant positions with the Company (persons that may be employed by the Company) (**Applicants**)	Full name, passport details and registration address for obtaining consent to the personal data processing, CV specifying previous jobs
The Company's employees with whom the Company has or had entered into employment contracts, including former employees with whom the employment contracts have been terminated (**Employees**)	Full name, passport details, INN, SNILS (personal pension account number), date of birth, gender, address of actual residence, home and mobile phone number, data for T-2 card: marriage status, previous jobs, data on employees' income at previous places of work (182-N certificate), language proficiency, military service obligation, family members, information on education, phone number, e-mail, address of actual residence, 2-NDFL and 182 certificates for the Accounting Department, employment record book, international passport data, data on coronavirus vaccination (certificates, QR codes) or medical exemption (doctor's excuse), a photo for internal use (to be taken on the first day of work), a photo for posting the information on corporate websites.
Close relatives and spouses of the Company's Employees whose personal data processing is provided for by law and is carried out by the Company as the employer in accordance with	Full name, date of birth, details of an identity document, address of residence, address of place of stay, contact phone number, individual amounts of insurance indemnity.

the requirements of state statistical authorities (**Employee's Relatives**)	
Contractors (individuals) who provide services for the Company and participants in exhibitions (**Counterparties**)	Full name, details of an identity document, SNILS, bank details, contact phone number, e-mail.
Representatives (individuals) of counterparties and customers of the Company with which the Company has or intends to establish contractual relations, including employees, owners, beneficiaries, representatives acting by virtue of a power of attorney and other representatives of counterparties (**Representatives of Company's Counterparties and Customers**)	Full name, place of work, passport number, driver's license number, job title, name of the structural unit, name of the current place of employment, address of the place of registration, time and date of visiting the premises, buildings and territory, data of the vehicle registration certificate; contact phone number and e-mail.
Persons who have registered on the ITE Connect platform (**Platform**) and persons who have not registered but use the Platform accessible through the website, mobile version of the website, applications and other resources (**Platform Users**) Platform addresses: ite-connect.com dairytech-connect.com aquatherm-connect.com airvent-connect.com mitt-connect.com mosbuild-connect.com transrussia-connect.com expoelectronica-connect.com securika-connect.com analitika-connect.com miningworld-connect.com rosupack-connect.com worldfood-connect.com weldex-connect.com	Full name, e-mail, phone number, gender, age, city and country of location, address of residence, citizenship and other data provided by Website Users and Platform Users while registering, filling out accounts (profiles) on websites and the Platform; data that is automatically transferred to the Company while using websites and the Platform with the software installed on the devices of Website Users and Platform Users (including the type of operating system, host IP address, sections of websites visited, cookies); data obtained as a result of the actions of Website Users and Platform Users on websites and the Platform.

yugagro-connect.com pharmtech-connect.com woodex-connect.com Visitors to the Company's websites in the Internet (**Website Users**)	
Participants in exhibitions held by the Company and their employees, as well as participants that submitted an application, but refused to participate (**Event Participants**)	Full name, position, phone number, e-mail, place of work, city and country of location; visited pages of and actions at websites.
Visitors to exhibitions held by the Company (**Exhibition Visitors**)	Full name, place of work, passport number, job title, name of the structural unit, current place of employment, pass (ID-card) identifier, address of the place of registration.
Company office visitors (**Office Visitors**)	Full name, data of vehicle registration certificate

2.2. To the extent required and sufficient for it to be classified as the personal data in accordance with the current legislation of the Russian Federation, any other data obtained by the Company is processed by the Company as the personal data upon the terms and conditions of this Policy.

3. Purposes of Personal Data Processing

3.1. The Company processes the personal data to achieve particular, predetermined and lawful purposes.

3.2. The Company processes the personal data in order to conduct its business as determined by the Charter and other by-laws of the Company, to perform the Company's obligations imposed on it by the current legislation, to perform signed contracts and for any other lawful purposes. The Company takes all steps required to comply with the requirements of the current legislation, does not process the personal data in cases where this is prohibited by law and is not required to achieve the purposes determined by the Company.

3.3. The purposes for which the Company processes the personal data in relation to certain categories of personal data subjects are, in particular:

3.3.1. Applicants: interviewing and deciding on possible filling vacancies that most fully meet the Company's requirements and including in the skill pool;

3.3.2. Employees:

- compliance with labour laws, including labour accounting and remuneration, making management and staff decisions on the employees, control over labour discipline;
- calculation and payment by the Company of wages, benefits and bonuses due to the employees, pension contributions and tax liabilities;
- performance by the Company of its social obligations to the employees and their relatives in the form of voluntary medical insurance, life insurance;
- execution of business trip documents for the Company's employees, booking and purchasing hotel accommodation and tickets for the Company's employees seconded on business trips;
- arranging for training for the Company's employees;
- ensuring the personal safety of the employees, other persons visiting real estate items (premises, buildings, territory) of the Company, as well as safeguarding of material and other valuables under the Company's supervision;
- provision by the Company of its employees with the corporate mobile communication service and ensuring efficient management and control of costs for that service;
- compliance by the Company with the requirements of labour laws on investigating and accounting for personal injuries that occur with the employees when they perform their labour functions and in any other cases provided for by labour laws.

3.3.3. Employee's Relatives:

- calculation and payment by the Company of wages, benefits and bonuses due to the employees, pension contributions and tax liabilities;
- performance by the Company of its social obligations to the employees and their relatives in the form of voluntary medical insurance, life insurance.

3.3.4. Counterparties (Individuals):

- supply of goods, performance of work and provision of services for the Company by its counterparties;
- providing temporary staff to work at exhibitions.

3.3.5. Representatives of Company's Counterparties and Customers (Legal Entities):

- supply of goods, performance of work and provision of services for the Company by its counterparties;
- arranging for and holding exhibitions and business program events as part of exhibitions (tenders, guided tours, internships, etc.);
- ensuring the personal safety of the employees, other persons visiting real estate items (premises, buildings, territory) of the Company, as well as safeguarding of material and other valuables under the Company's supervision.

3.3.6. Website Users and Platform Users:

- registering and signing in on the websites and the Platform;
- operation of the websites and the Platform;
- providing information on the events held;
- interaction among Event Participants and Exhibition Visitors;
- checking in for the events;
- exhibition feedback;
- print media accreditation;
- advertising and promoting the exhibitions.

3.3.7. Event Participants:

- arranging for and holding exhibitions and business program events as part of exhibitions (tenders, guided tours, internships, etc.);
- advertising and promoting the exhibitions.

3.3.8. Visitors:

providing information on the events held;

checking in for the events;

exhibition feedback;

advertising and promoting the exhibitions.

4. Legal Grounds for Personal Data Processing

4.1. The legal grounds for the personal data processing by the Company are, in particular:

4.1.1. Consent of the personal data subject to the processing of their personal data. The procedure for the Company obtaining the consent of the personal data subject is determined by section 5 of the Policy.

4.1.2. Federal laws of the Russian Federation and regulatory legal acts adopted on the basis thereof, in particular:

- Labour Code of the Russian Federation;
- Civil Code of the Russian Federation;
- Tax Code of the Russian Federation;
- Federal Law On Personal Data No. 152-FZ dated 27 July 2006;
- Federal Law On Individual (Personalized) Accounting in the Compulsory Pension Insurance System No. 27-FZ dated 01 April 1996;

- Federal Law On Compulsory Pension Insurance in the Russian Federation No. 167-FZ dated 15 December 2001;
- Federal Law On Archive-Keeping in the Russian Federation No. 125-FZ dated 22 October 2004;
- Federal Law On Information, Informational Technologies and Information Protection No. 149-FZ dated 27 July 2006;
- Federal Law On Accounting in the Russian Federation No. 402-FZ dated 06 December 2011;
- Federal Law On State Registration of Legal Entities and Individual Entrepreneurs No. 129-FZ dated 08 August 2001;
- Decree of the Government of the Russian Federation On Approval of Requirements for the Protection of Personal Data while Processing it in Personal Data Information Systems No. 1119 dated 01 November 2012;
- Decree of the Government of the Russian Federation On Approval of Regulations on Specific Features of Processing Personal Data without Computer-Aided Facilities No. 687 dated 15 September 2008.

4.1.3. The Charter and other by-laws governing the Company's business.

4.1.4. The Company's by-laws governing issues related to the personal data processing.

4.1.5. Contracts entered into between the Company and personal data subjects. Such contracts are, without limitation, employment contracts with the Employees in accordance with the Labour Code of the Russian Federation, civil law contracts with the counterparties and contracts entered into with Website Users and Platform Users, in particular, the Platform Use Rules (**Rules**).

5. Consent of a Personal Data Subject to Personal Data Processing

5.1. The personal data subject decides to provide their personal data to the Company and consents to its processing freely, wilfully and to their own benefit. The consent to the personal data processing is particular, focused, informed, conscious and unambiguous and may be granted by the subject in any form that enables to confirm its receipt, unless otherwise provided for by law.

5.2. The law provides for certain cases when the consent of the personal data subjects must be obtained in writing:

5.2.1. Transfer of the Employees' personal data to any third parties, including legal entities that carry out HR recordkeeping and/or accounting on behalf of the Company; transfer of the Employee's personal data when booking hotel accommodation and tickets (in cases not related to the performance of employment duties by the Employee); transfer of personal data to banks that open and maintain payment cards for accruing wages and other income of the Employee, insurance companies that provide voluntary medical and pension insurance, accident insurance of the Employees at the expense of the Company

as the employer, entities that arrange for treatment and recreation of the Employees and their family members, printing companies engaged in the manufacture of Employees' business cards, etc.

5.2.2. Processing of special categories of personal data of any personal data subjects relating to race, nationality, political views, religious or philosophical beliefs, health, intimate life, including the processing of information on the Employee's health not related to the Employee's ability to perform their labour function and not required to achieve the purposes provided for by the pension laws.

5.2.3. Processing of biometric personal data (the data that describes the physiological and biological features of the person on the basis whereof their identity may be established and which is used for this purpose) of any personal data subjects.

5.2.4. Cross-border transfer of personal data of any personal data subjects in the territory of foreign states that do not ensure proper protection of the rights of personal data subjects (e.g., the United States).

5.2.5. Obtaining personal data of the Employees from any third parties, including for the purpose of its verification and in cases where such data cannot be obtained from the Employee.

5.2.6. Making decisions that give rise to legal effects for the personal data subject or otherwise affect their rights and lawful interests based on automated processing of the subject's personal data only.

5.2.7. Inclusion of the personal data of subjects in public sources of personal data (e.g., posting it on the corporate portal),

5.3. The dissemination of personal data of subjects (e.g., posting the data on corporate websites) requires a separate consent to the data processing in accordance with Article 10.1. of Federal Law On Personal Data No. 152-FZ dated 27 July 2006.

5.4. A model Employee's written consent to the processing of their personal data by the Company is in ***Appendix No. 1*** to the Policy. Model consents to the personal data dissemination are in ***Appendix No. 2*** (Employees) and ***Appendix No. 3*** (experts, event speakers, other persons).

5.5. As a general rule, the Employee's express consent to the processing of their personal data is not required if the processing is required to perform the employment contract which party is the Employee being the personal data subject. The written consent of the Employee is required to transfer their personal data to any third parties and other particular cases of personal data processing (as enumerated in Clause 5.2 of the Policy above).

5.6. No express consent of Relatives of the Company's employees is required if their personal data is processed on the basis of federal laws (to accrue alimony, provide social payments, fringe benefits and guarantees, etc.), by the Company as the employer in accordance with the requirements of state statistical authorities and if the Employee's Relative is a beneficiary under a contract with the Company. In all other cases, it is necessary to obtain a provable (confirmed) consent of the Employee's Relatives for the processing of their personal data by the Company.

5.7. As a general rule, the Applicant's express consent to the processing of their personal data is not required if the Applicant has themselves sent to the Company's their CV by e-mail (or in any other way) or posted it on the Internet for the general public. In these cases, it is deemed that by their implicative actions, the Applicant has granted their consent to the processing of their personal data by the Company. At that, the Company takes additional steps aimed at confirming the fact that a particular applicant has sent their CV (feedback by e-mail, phone, etc.).

5.8. The Applicant's written consent must be obtained only in particular cases of personal data processing as enumerated in Clause 5.2. of the Policy above.

5.9. If a decision is made to refuse to hire the Applicant, their personal data must be destroyed within 30 days from the date such decision is made, unless otherwise provided for by the agreement with the Applicant or specified in their consent to the personal data processing. To enable the processing of candidates' CVs after the specified period, it is necessary to execute the candidate's consent in the form of ***Appendix No. 4*** to this Policy.

5.10. The Company's Websites Users grant their consent to the processing of their data by ticking the electronic consent form.

5.11. By registering on the Platform, the Platform Users agree to this Policy.

5.12. The Company processes the Platform Users' personal data in order to comply with the Rules, therefore, the Platform Users' consent to the processing of their personal data is not required by virtue of the provisions of the personal data laws.

5.13. The Company processes the Website Users' personal data in order to provide them with access to the functionality of the Company's websites. The Company processes the Platform Users' personal data in order to perform its obligations to provide them with access to the Platform and its functionality.

5.14. The Company has no purpose to and does not process any biometric data and any special categories of data of the Website Users and the Platform Users.

5.15. As a general rule, there is no need to obtain the consent to processing in relation to the Individual Counterparties, if there is a contract with the Company and if the subjects independently send their personal data to the Company or its Employees and thereby take implicative actions that confirm their consent to the processing of such personal data by the Company.

5.16. If the Company obtains any personal data from its Counterparties being legal entities on the basis of a contract entered into with them, the counterparty transferring the personal data is liable for the legality and reliability of the personal data and for obtaining the consent of personal data subjects to their personal data transfer to the Company, if such obligation is directly stipulated by the contract with it. In this case, the Company does not assume the obligation to inform the subjects (their representatives) whose personal data is transferred to it, on the commencement of personal data processing, as it is the counterparty that transfers the personal data that incurs the obligation to inform when a contract is entered into with the personal data subject and/or the consent to such transfer is obtained.

5.17. The personal data of persons who have signed contracts with the Company that is contained in the Unified State Registers of Legal Entities and Individual Entrepreneurs is open and publicly available, except for the number, date of issue and the authority that issued the identity document of an individual. The publicly available data must not be kept confidential, and no consent of the personal data subjects for its processing is required.

5.18. The consent of Event Visitors and Event Participants to the processing of their personal data is provided in the form of implicative actions of those subjects that send their personal data to participate in the event and thereby confirm their consent to its processing by the Company and by ticking when filling out the questionnaire at the Company's website or in hard copy, as well as in the form of implicative actions by transferring their business cards to the Company's representatives as part of their participation in the event.

5.19. The consent of the Company's Office Visitors to the processing of their personal data is provided in the form of implicative actions, i.e. by showing an identity document and providing the information requested from them when they visit the Company's offices.

5.20. No consent of the Employees to provide their personal data is required when the Company receives, within the established powers, any reasoned requests from prosecutors, law enforcement agencies, investigation and inquiry agencies, security agencies, state labour inspectors when they exercise state supervision and control over compliance with the labour laws and other bodies authorised to request information within the jurisdiction provided for by law.

5.21. A reasoned request should include its purpose, a reference to its legal grounds, including those confirming the authority of the body that sent the request and a list of the information requested.

5.22. In the event that any requests are received from any entities that do not have the respective authority, the Company must obtain the Employee's consent to the provision of their personal data in any provable form and warn the persons receiving the personal data that such data may be used solely for the purposes for which it is reported and require those persons to confirm that such rule will be (was) observed.

5.23. The consent to the processing of personal data the processing whereof is not established by the requirements of law or is not required to perform the contract with the Company which party is the personal data subject may be revoked by the personal data subject. In this case, the Company destroys such personal data in respect whereof the consent to processing is revoked and ensures their destruction by the counterparties that processed such data on behalf of the Company within Thirty (30) calendar days from the date the revocation of the subject's consent to the processing of their personal data is received.

5.24. In accordance with Federal Law On Personal Data No. 152-FZ dated 27 July 2006, the Company may process the personal data without obtaining the subjects' consent in certain cases, e.g., when processing:

- personal data for statistical or other research purposes, provided that the personal data must be depersonalised;

- personal data access whereto is provided to the general public by the personal data subject or at their request.

5.25. In all cases, the Company must prove that the consent has been obtained of the personal data subject to the processing of their personal data or that there are grounds for processing the personal data without the consent as specified in Federal Law On Personal Data No. 152-FZ dated 27 July 2006.

6. Procedure and Conditions for Personal Data Processing

List of Actions and Ways of Personal Data Processing

6.1. The Company processes the personal data by taking various actions provided for by the current legislation (collection, systematisation, accumulation, storage, clarification (updating or modification), use (including transfer), depersonalisation, blocking, destruction of personal data, etc.).

6.2. The Company processes the personal data with and without computer-aided facilities.

6.3. The Policy applies in full to the personal data processing with the computer-aided facilities and if the personal data is processed without the computer-aided facilities, solely in cases where such processing matches the nature of actions (operations) taken in relation to the personal data with the computer-aided facilities, i.e. enables to search by an algorithm for the personal data recorded on a tangible medium and contained in file cabinets or any other systematised collections of personal data and/or to access such personal data.

6.4. The Company takes all reasonable steps to keep up-to-date the personal data processed, including, but not limited to, the exercise of each subject's right to receive their personal data for review and to require the Company to clarify, block or destroy it if the personal data is incomplete, outdated, inaccurate, illegally obtained or is not required for the processing purposes stated above.

Conditions for Personal Data Transfer to any Third Parties

6.5. The Company does not disclose to any third parties and does not disseminate the personal data without the consent of the personal data subject, unless otherwise provided for by law or a contract with the personal data subject.

6.6. Unless otherwise provided for by law, the Company may instruct another person to process the personal data on the basis of a contract entered into with that person.

6.7. The commission contract for the personal data processing entered into by the Company provides as a material condition for the obligation of the person processing the personal data on behalf of the Company to comply with the principles and rules for the personal data processing provided for by law, to keep the personal data confidential and to take the necessary steps aimed at ensuring the performance of the obligations stipulated by law.

6.8. The scope of personal data transferred to another person for processing and the ways of processing are the baseline minimum for such person to perform its obligations to the Company.

6.9. The Company's commission contract determines the list of personal data, the list of actions (operations) therewith that will be taken by the person processing the personal data and the purposes of its processing. The Company's commission contract establishes the obligation of the person processing the personal data on its behalf to keep the personal data confidential, the requirements provided for by Part 5 of Article 18 and Article 18.1 of Federal Law On Personal Data No. 152-FZ dated 27 July 2006, the obligation to provide documents and other information confirming that the steps are taken and the requirements established by law are complied with in order to perform the Company's commission at the Company's request during the term of the Company's commission, including prior to the personal data processing, the obligation to secure the personal data while processing it, and specifies the requirements to protect the personal data processed in accordance with Article 19 of Federal Law On Personal Data No. 152-FZ dated 27 July 2006, among other things, to notify the controller of the cases provided for by Part 3.1 of Article 21 of Federal Law On Personal Data No. 152-FZ dated 27 July 2006.

6.10. When fulfilling the Company's commission to process the personal data, the person instructed to process may use its information systems located in the Russian Federation and meeting the security requirements established by law in order to process the personal data; this is recorded by the Company in the signed commission contract for the personal data processing.

6.11. If the Company instructs another person to process the personal data, the Company is liable for the actions of that person to the personal data subject. The person that processes the personal data on behalf of the Company is liable to the Company.

Location of Databases Containing Personal Data of Citizens of the Russian Federation

6.12. When collecting the personal data, the Company ensures that the personal data of citizens of the Russian Federation is recorded, systematised, accumulated, stored, clarified (updated, modified), retrieved by using databases located in the Russian Federation. If the Company does not have information on the citizenship of the personal data subject, the Company proceeds from the fact that all data received in the Russian Federation was received from citizens of the Russian Federation.

Cross-Border Transfer

6.13. The Company may transfer the personal data of Applicants and Employees across the border to its affiliates that are members of ITE Group, in particular to the UK. The purposes of such cross-border transfer are: to resolve issues related to the employment of Applicants, to provide the Employees with access to corporate information systems, to appraise the Employees, to jointly arrange for events, etc. The personal data is transferred to the extent required to achieve the purposes. The personal data processing by the persons that received it as a result of cross-border transfer is automated and includes accumulation, storage, clarification (updating or modification), use,

depersonalisation, blocking and destruction. The persons processing the personal data as a result of cross-border transfer are subject to the requirements for storage and protection of personal data similar to those established by the Company.

6.14. The United Kingdom is a party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. ETS-108 and is included in the list of foreign states recognised by Roskomnadzor as those that properly protect the personal data subjects' rights, therefore, the cross-border transfer to the UK may be carried out in accordance with the law during the period when a notice of intent to carry out the cross-border transfer is considered.

Special Categories of Personal Data and Biometric Personal Data

6.15. The Company does not process any personal data on race, nationality, political views, religious or philosophical beliefs, intimate life, membership in public associations or trade union activities of the Employees, except as expressly provided for by law or where such information is posted on publicly available sources, including the Company's internal corporate portal.

6.16. The personal data on a criminal record may be processed by the Company only in cases and in the manner prescribed by law.

6.17. The Company does not process any biometric personal data.

Restrictions on the Personal Data Storage Period

6.18. The Company stores the personal data in a form that enables to identify the personal data subject no longer than required for the purposes of personal data processing, unless a different period of personal data storage is established by law, a contract which party is the personal data subject and the consent of the personal data subject to data processing.

6.19. The general periods of storage and/or the conditions for destruction of the personal data are established in the List of Personal Data Processed by the Company as approved by the Company's Director General (the form of the List is in ***Appendix No. 5*** to the Policy).

6.20. After the purposes of processing the personal data are achieved (or in case there is no need to achieve them any more), if the Company is not able to cure the violations of the procedure for the personal data processing established by law, and in case the consent is revoked by the personal data subject or the period expires for the personal data processing as established by the consent to the personal data processing, unless otherwise provided for by law or contracts with the personal data subjects, the Company destroys or depersonalises such personal data or transfers it to archival storage in cases provided for by the current legislation and in accordance with the established procedure.

7. Confidentiality of Personal Data

7.1. The Company's Employees who have access to the personal data must keep such data confidential.

The following data must not be kept confidential:

- personal data after it is depersonalised;
- publicly available personal data.

7.2. The Company may host its personal data information systems in a data centre or a cloud computing infrastructure. If the contract with the data centre prohibits access of the data centre staff to the processed data of the Company, the Company does not treat such hosting as a commission to the data centre to process the personal data and does not request the consent of personal data subjects. In all cases, the contract with the data centre (provider) contains the requirements for confidentiality and security of the personal data processed.

8. Rights of Personal Data Subjects

8.1. The personal data subject has the right to receive information on the processing of their personal data that contains, among other things:

- the confirmation that their personal data is processed by the Company;
- legal grounds and purposes of personal data processing;
- information on the ways of personal data processing used by the Company;
- name and location of the Company, information on the persons (except for the Company's employees) who have access to the personal data or whom the personal data may be disclosed to on the basis of a contract with the Company or the provisions of law;
- the personal data processed that relates to the respective personal data subject, the source of its receipt;
- the personal data processing period, including the storage period;
- procedure for exercising by the personal data subject of their rights provided for by Federal Law On Personal Data No. 152-FZ dated 27 July 2006;
- information on a completed or expected trans-border transfer of the data;
- name or name, patronymic, last name and address of the person processing the personal data on behalf of the controller, if that person is or will be instructed to process;
- any other information provided by law.

8.2. The information on availability of personal data must be provided to the personal data subject by an authorised employee of the Company in an understandable form and it should not contain any personal data related to any other personal data subjects. A model response to subject's requests regarding the processing of their personal data is in ***Appendix No. 6*** to the Policy.

8.3. The subject's request regarding the processing of their personal data by the Company may be made electronically or in hard copy. The electronic form is allowed if the request is made in the form of an electronic document signed with a digital signature or made through the personal data subject's account at the Company's website (in this case, the use of a login and password combination is treated as a simple digital signature, as it confirms that the message is sent by a particular person).

8.4. The personal data subject's request must contain:

- last name, name and patronymic of the personal data subject or their representative;
- number of the primary identity document of the personal data subject and of their representative (if the request is sent by the representative), date of issue of that document (those documents) and the body(ies) that issued it (them);
- information confirming the relations of the personal data subject with the Company (number and date of the contract entered into with the Company and/or other information, a copy (scan, photo) of the message in the form of a letter, an SMS message or in electronic form received from the Company etc.), or information otherwise confirming that the personal data is processed by the Company;
- signature of the personal data subject or their representative.

8.5. All requests received from the personal data subjects or their representatives are registered in accordance with the procedure established by the Company, reported to the person responsible for the personal data processing at the Company and sent upon his/her resolution to the respective structural unit of the Company for drawing up a response as soon as possible.

8.6. If the information specified in Clause 8.1 of the Policy and the personal data processed were provided for review by the personal data subject at their request, the personal data subject may contact the Company once again or send a second request in order to obtain such information and to review their personal data not earlier than 30 days after the initial message or the initial request, unless a shorter period is established by law, a regulatory legal act adopted in accordance therewith or a contract which party or beneficiary is the personal data subject.

8.7. A repeated request of the personal data subject is to be fulfilled earlier that the period provided for by Clause 8.6 expires if such information and/or personal data processed were not provided to the subject for review in full by results of consideration of the initial message. The repeated request of the personal data subject and the information specified in Clause 8.4 must contain the rationale for sending the repeated request.

8.8. If the request is received from the personal data subject in hard copy, in order to identify the personal data subject, the Company may request from such person additional information provided by the personal data subject when registering at the Company's website or the Platform or ask that person to send an electronic request through the respective account (profile) of the personal data subject at the Company's website or the Platform. If the contacting person fails to take those additional actions, the Company

may refuse to provide such person with the requested information on the personal data processing in order to protect the rights of third parties and to prevent unauthorised disclosure of personal data of such persons.

8.9. If the subject's request does not contain the information specified in Clause 8.4 of the Policy or the time limits and conditions specified in Clauses 8.6 and 8.7 of the Policy are not met, the Company may refuse to provide the subject with the information requested. The form of refusal to fulfil the personal data subject's request is in ***Appendix No. 7*** to the Policy.

8.10. The personal data subject may require the Company to clarify, block or destroy their personal data, if the personal data is incomplete, outdated, inaccurate, unreliable, unlawfully obtained or not required for the stated purpose of processing, and may take steps to protect their rights as provided for by law. The subject's request must be submitted in writing or electronically, specify the information on the identity document or the personal data specified by them when they provide their personal data to the Company, including when they fill out questionnaires in order to complete surveys or to register at the website, and identify them. The Company's employees execute such request as a written application in any form.

8.11. The subject may revoke their consent to the personal data processing by the Company at any time by submitting a written application in any form that contains information on the primary identity document of the subject or the same personal data that was specified when the personal data was provided to the Company. In this case, if the consent to the personal data processing was initially provided by the subject in electronic form at the Company's website or by accepting the Rules at the Platform:

- such consent may be revoked both in hard copy and electronically through the account (profile) of the respective User of the Company's website or the Platform User;
- If the revocation is received in hard copy, in order to identify the personal data subject, the Company may request from such person additional information provided by the personal data subject when registering at the Company's website or the Platform or ask that person to send an electronic request for consent revocation through the respective account (profile) of the personal data subject at the Company's website or the Platform. If the contacting person fails to take those additional actions, the Company may refuse such person to revoke their consent to the personal data processing in order to protect the rights of third parties.

8.12. In the event that the personal data subject revokes their consent to the personal data processing, the Company may continue to process the personal data without the consent of the personal data subject if there are grounds provided for by law.

8.13. In the event that the subject revokes their consent to the processing of their personal data, if there are no legal grounds to continue its processing, the Company ceases to process it (ensures that the persons instructed by the Company to process it cease its processing) and destroys or depersonalises (ensures the destruction or depersonalisation) of the personal data within 30 days from the date such revocation is received.

8.14. If the personal data subject sends the Company the message to cease the personal data processing, the Company ceases to process it or ensures that such processing ceases (if such processing is carried out by the person processing the personal data) within 10 business days from the date the respective request is received, except as provided for by law. The Company reserves the right to send to the personal data subject a reasoned notice that this period is extended for no more than 5 business days, specifying the reasons for such extension.

8.15. If the personal data subject believes that the Company processes their personal data in violation of the requirements of law or otherwise violates their rights and freedoms, the personal data subject may appeal against the Company's actions or inaction to the body authorised to protect the personal data subjects' rights (Roskomnadzor) or to court.

8.16. The personal data subject has the right to protect their rights and lawful interests, including reimbursement for loss and/or compensation for moral harm in court.

9. Obligations of the Company

9.1. When collecting the personal data, the Company must provide the personal data subject at their request with the information stipulated by Clause 8.1 of the Policy.

9.2. The Company must inform the personal data subject or their representative on the availability of personal data relating to the respective personal data subject and to grant the opportunity to review that personal data free of charge when the personal data subject or their representative contacts the Company within 10 days from the date the request of the personal data subject or their representative is received. The Company reserves the right to send to the personal data subject a reasoned notice that this period is extended for no more than 5 business days, specifying the reasons for such extension.

9.3. The Company must change the personal data accordingly within 7 business days from the date the personal data subject or their representative provides the information confirming that the personal data is incomplete, inaccurate or out of date.

9.4. If any inappropriate personal data processing is identified when the personal data subject or their representative contacts the Company or at the request of the personal data subject, or their representative, or the body authorised to protect the personal data subjects' rights, the Company must block the inappropriately processed personal data relating to that personal data subject or ensure its blocking (if the personal data is processed by another person acting on behalf of the Company) from the time of such contact or of the receipt of such message for the period of check.

9.5. In the event that any inaccurate personal data is identified and the personal data subject or their representative contacts the Company in this regard, or at their request or at the request of the body authorised to protect the personal data subjects' rights, the Company must block the personal data relating to that personal data subject or ensure its blocking (if the personal data is processed by another person acting on behalf of the Company) from the time of such contact or of the receipt of that message for the period of check, unless the personal data blocking violates the rights and lawful interests of the personal data subject or any third parties.

9.6. If the inaccuracy of the personal data is confirmed on the basis of information provided by the personal data subject or their representative, or the body authorised to protect the personal data subjects' rights. or other necessary documents, the Company must clarify the personal data or ensure that it is clarified (if the personal data is processed by another person acting on behalf of the Company) within 7 business days from the date such information is submitted and stop blocking the personal data.

9.7. In case any inappropriate personal data processing is identified that is carried out by the Company or a person acting on its behalf, the Company must stop the inappropriate personal data processing or ensure that it is stopped by the person acting on behalf of Company, within 3 business days from the date it is identified.

9.8. If it is impossible to ensure that the personal data processing is appropriate, the Company must destroy such personal data or ensure their destruction within 10 business days from the date the inappropriate personal data processing is identified. The Company must notify the personal data subject or their representative of curing the violations or destroying the personal data, and if the message of the personal data subject or their representative or the request of the body authorised to protect the personal data subjects' rights were sent by the body authorised to protect the personal data subjects' rights, the Company must notify that body as well.

9.9. If the personal data was not received from the personal data subject, the Company must provide the personal data subject with the following information before using such personal data:

- name and address of the Company;
- purpose of and legal grounds for the personal data processing;
- list of the personal data;
- expected users of the personal data;
- rights granted to the personal data subjects under Federal Law On Personal Data No. 152-FZ dated 27 July 2006;
- the source of obtaining the personal data.

9.10. The personal data subject is not required to be informed of the Company's receipt of and intention to process their data in the following cases:

- the personal data subject has already been notified of their personal data processing by the respective controller;
- the personal data is received by the Company due to the performance of a contract which party is the personal data subject;
- the personal data is made publicly available by the personal data subject or obtained from a publicly available source;
- The Company processes the personal data for statistical or other research purposes, unless the rights and lawful interests of the personal data subject are violated;

- the provision of the personal data subject with the information specified in Clause 8.3 of the Policy violates the rights and lawful interests of any third parties.

9.11. In cases where the personal data must be provided and/or the Company must obtain the consent to the personal data processing in accordance with the law, the Company must explain to the personal data subject the legal effects of the personal data subject's refusal to provide their personal data and/or to consent to its processing by the Company. A model form for explaining the effects of refusing to provide the personal data is in ***Appendix No. 8*** to the Policy.

10. Arranging for Personal Data Processing

10.1. **Person Responsible for the Personal Data Processing**

10.1.1. The Company appoints a person responsible for arranging for the personal data processing.

10.1.2. The person responsible for arranging for the personal data processing receives instructions on these issues directly from the Director General of the Company and is accountable to him/her.

10.1.3. The heads of the Company's structural units must promptly provide the necessary materials and information at the request of the person responsible for arranging for the personal data processing and to cure violations of the requirements of law for handling the personal data if such violations are identified at the Company's unit.

10.1.4. The person responsible for arranging for the personal data processing must:

- exercise internal control over the compliance by the Company and its employees with the personal data laws of the Russian Federation, including the requirements for the protection of personal data;
- bring to the attention of the Company's employees provisions of the personal data laws of the Russian Federation, the Company's personal data processing by-laws and the requirements for the protection of personal data;
- arrange for and/or exercise control over the receipt and handling of messages and requests of the personal data subjects or their representatives by the structural units of the Company.

10.2. **Authorisation System of Access to Personal Data**

10.2.1. The Company's employees who need access to the personal data in order to perform their employment (labour) duties may access the respective personal data in accordance with the List of Positions of the Company's Employees which Involve the Processing of or Access to the Personal Data as approved by the Director General of the Company and put into effect by his/her order (the form of the List of Positions is in ***Appendix No. 9*** to the Policy).

10.2.2. The List of Positions of the Company's Employees which Involve the Processing of or Access to the Personal Data, consists of two parts, i.e. a fixed and a variable one. The fixed part of the List determines the positions of employees of the Company's structural

units and the number of employees holding those positions who need access to the personal data in order to perform their labour duties. The variable part specifies the last names and initials of the employees holding the respective positions.

The List of Positions is kept by the HR service. The List of Positions may be kept (the information of the variable part may be filled in) electronically.

The List of Positions is to be amended as often as required (when the staff schedule or the business processes of the Company change) by order of the Director General of the Company.

10.2.3. The Company's employee whose position is not included in the List of Positions of the Company's Employees which Involve the Processing of or Access to the Personal Data, but who needs one-time or temporary access to the personal data of the personal data subjects due to the performance of their employment duties, may be granted such access on the basis of a written application of the immediate supervisor of the Employee to the attention of the Director General of the Company. The form of this application is in ***Appendix No. 10*** to the Policy.

10.2.4. The Company's employees are granted access to that personal data only that they need to perform their employment duties.

To this end, particular Employees are entrusted with the storage and use of tangible media of the personal data, and the access rights of users are segregated in the information systems.

10.2.5. The duties of persons that may handle the personal data are determined by the respective sections of their job descriptions/employment contracts. A model section of the job description/employment contract that governs the handling of personal data is in ***Appendix No. 11*** to the Policy.

10.3. **Handling the Personal Data**

10.3.1. Each copy of all tangible media of the personal data must be accounted for.

10.3.2. The machine media of personal data (hard drives of servers and workstations, optical discs, removable drives, tapes (cassettes) for backup, etc.) are accounted for in the form established by ***Appendix No. 12*** to the Policy. In the event that the machine media are embedded in the servers, workstations, systems and data storage networks, the media are accounted for without their removal from the technical facility by specifying the respective data in column 5 of the Machine Media Log. The information on the media (their type and capacity) is entered on the basis of data obtained using the standard tools of the operating system or the respective application.

10.3.3. The personal data media in hard copy are accounted for in the form established for registration of the Company's documents and as per the forms established for particular types of personal data media (personal records, employment record books, contracts of the Company, etc.).

10.3.4. The files containing the personal data, including scans of documents with the personal data, may be recorded and stored only in network storages (on file servers, network drives and in network directories/folders) that are specially intended for these purposes.

The list of such network storages is determined in the in-house regulations of the Company.

10.3.5. It is prohibited to record and store the personal data on any other hard and network drives, including hard drives of user workstations, and on any other machine media that are not accounted for in accordance with the above procedure.

10.4. **Personal Data Storage**

10.4.1. The personal data must be stored in a form that enables to identify the personal data subject no longer than required for the purposes of personal data processing, unless a particular period of personal data storage is established by law, a contract which party is the personal data subject or the consent of the personal data subject to the personal data processing. The general periods for storing the personal data and/or the conditions for its destruction are established by the List of Personal Data Processed by the Company in Personal Data Information Systems and without Computer-Aided Facilities as approved by the Director General of the Company.

10.4.2. The personal data processed is to be destroyed or depersonalised when the processing purposes are achieved or in case there is no need to achieve them any more, the consent of the personal data subject to the processing of their personal data is revoked or it is transferred to archival storage in cases provided for by law and regulatory legal acts of the federal executive authorities authorised to govern the archival storage.

10.4.3. The transfer of documents containing the personal data to and the time limits for their archival storage are determined by the respective laws and regulatory legal acts of the authorised federal executive authorities.

10.4.4. The personal data of the Website Users and the Platform Users is processed and stored in the Russian Federation. The storage is to be on electronic media only, and the personal data is to be processed with and without the use of automated systems.

10.4.5. The Website Users' consent to the processing is stored for no more than 3 years after the consent expires. Other documents and information: until the purpose of processing is achieved.

10.4.6. The personal data of each Platform User is stored until the purposes of their processing are achieved, i.e., during the period the Rules are in effect for a particular User, and after the Rules expire, for the period required and established by the current legislation of the Russian Federation.

10.4.7. If the Platform User deletes their account (profile), the Company stores the necessary personal data of the Platform User on its electronic media during the period required and established by the current legislation of the Russian Federation.

10.5. **Personal Data Destruction**

10.5.1. The Company destroys the personal data in respect whereof:

- the purpose of processing the personal data is achieved;
- there is no need to achieve the purposes of processing determined earlier;

- any inappropriate personal data processing is identified (including in case the personal data subject contacts), when it is not possible to ensure that it is processed appropriately;
- the subject's consent to the personal data processing is revoked, and there are no legal grounds to continue such processing;
- there are no grounds for archival storage of the tangible media containing that personal data;
- the term for processing the personal data provided for by the consent of the personal data subject expires.

In cases where the personal data is expected to be used for the purposes of further analysis, statistical recording, research, they may be depersonalised by the Company in a way that renders it impossible to attribute it to a particular personal data subject in accordance with the requirements of Roskomnadzor Order On Approval of Requirements for and Ways of Personal Data Depersonalising No. 996 dated 05 September 2013.

10.5.2. In order to destroy the tangible media of personal data or to transfer it to archival storage, a respective board is appointed by order of the Company. The board members are determined by the person responsible for the personal data processing.

10.5.3. The board chooses the tangible media of personal data to be destroyed or transferred to archival storage, determines the data to be destroyed / transferred and destroys it after the list of documents and data is approved by the person who appointed the board.

The tangible media subject to archival storage are transferred under the certificate to the structural unit of the Company which is entrusted with the archiving or to a third-party entity engaged for those purposes.

10.5.4. The destruction of tangible media of the personal data must ensure that they are physically destroyed in full and the destruction of the personal data recorded on machine media must ensure as well that the personal data may not be recovered.

10.5.5. A part of the personal data may be destroyed or depersonalised (if possible using a particular tangible medium) by means preventing further processing of such personal data while enabling to process other data recorded on the tangible medium (deletion, defacement).

10.5.6. The personal data must be destroyed within 10 business days from the date the data to be destroyed is revealed. In all cases, the period of destruction must not be more than 30 days from the date the period of storage of the personal data expires, the purposes of processing the personal data are achieved, there is no need to achieve those purposes any more, the subject's consent to the personal data processing is revoked or any inappropriate processing of the personal data is identified, unless otherwise provided for by law.

10.5.7. If the personal data may not be destroyed within the period specified in Clause 10.5.6., the Company blocks such personal data or ensures blocking thereof (if the personal data

is processed by another person acting on behalf of the Company) and destroys the personal data thereafter within 6 months, unless any other period is established by law.

10.5.8. Any machine media containing the personal data that have got out of order, time-expired or lost their practical importance are destroyed by the Company in one of the following ways: cutting, burning, mechanical destruction, handing over to a company that recycles recoverable resources. In the latter case, before the machine media are handed over for recycling, the Company erases the personal data on all media using programs (devices) for assured destruction of information.

10.5.9. Any media in hard copy are destructed using shredding machines, by burning or handing them over to a company that recycles recoverable resources for subsequent destruction.

10.5.10. In the event that the tangible media are destroyed by a designated company that recycles recoverable resources, the contract with such company should provide that it must keep confidential the personal data on the media being destroyed (recycled). If such obligation is not provided for by the contract, the destruction must be carried out under the personal supervision of an authorised employee of the Company only.

10.5.11. The personal data is destroyed in the information systems by deleting database records that contain the personal data or by erasing files using programs (devices) for assured destruction of information.

10.5.12. By results of the destruction, a certificate of personal data destruction is to be drawn up that must contain the following information: data that identifies the subject whose personal data was destroyed, the composition of the destroyed data, the list of information systems where the data was destroyed (***Appendices No. 13*** and ***14*** to the Policy).

10.5.13. Any tangible media of personal data that are in archival storage, personal data contained in electronic archives, archival copies of databases containing destroyed personal data are to be destroyed in accordance with the rules of the archiving laws of the Russian Federation.

11. Data on Steps Taken to Protect Personal Data

11.1. Steps to secure the personal data are an integral part of the Company's activities.

11.2. The work to secure the personal data is arranged for by the management of the Company.

11.3. The development and taking of steps to secure the personal data while it is processed with computer-aided facilities is imposed on the person responsible for the personal data processing at the Company and/or the person responsible for securing the personal data in the personal data information systems.

11.4. In order to choose and implement methods and means of protecting the information (personal data), an entity may be engaged that has a duly issued license for the technical protection of confidential information and other licenses, as established by law and required to perform particular work.

11.5. The personal data is secured by the Company by preventing any unauthorised, including accidental, access thereto which may result in the destruction, modification, blocking, copying, dissemination of the personal data and any other unauthorised actions.

11.6. The personal data processed by the Company is secured by taking legal, organizational and technical measures that are required and sufficient to comply with the requirements of the personal data laws.

11.7. The legal measures taken by the Company include:

- development of the Company‘s by-laws that implement the requirements of law, including this Policy;
- not using any methods of processing the personal data that are contrary to the purposes defined by the Policy and the requirements of law.

11.8. The organizational measures taken by the Company include:

- appointment of the person responsible for the personal data processing;
- limiting the number of the Company’s employees who have access to the personal data, arranging for an authorisation system for access thereto, identifying and authenticating access subjects and access objects, managing and segregating such access;
- issuing the personal data processing by-laws;
- the Company’s employees who directly process the personal data must read, understand, and acknowledge by signing the provisions of the personal data laws, including the requirements for the personal data protection, the Policy, any other by-laws of the Company on the personal data processing;
- training all categories of the Company’s employees who directly process the personal data on the rules for its handling and securing the data processed;
- establishing the obligations to secure the personal data processing and liability for a violation of the established procedure in the job descriptions and/or employment contracts (additional agreements thereto) with the Company’s employees;
- personal data processing regulation;
- arranging for accounting for and storage of the tangible media of personal data that prevent theft, substitution, unauthorised copying and destruction;
- identification of personal data security threats while processing such data in the information systems and threat modelling on the basis thereof;
- data processing hardware placement within a protected area;
- restricting third-party access to the Company’s premises, preventing them from accessing premises in which personal data is processed and processing hardware is located without supervision on the part of the Company’s employees.

11.9. The technical measures taken by the Company include:

- determining the type of personal data security threats that are relevant to the personal data information systems, subject to the assessment of potential harm that may be caused to the personal data subjects in case the security requirements are violated, determining the level of personal data protection and the requirements for the personal data protection while processing it in the information systems, the compliance wherewith ensures the established levels of personal data protection;
- development of a personal data protection system based on the threat model for the levels of personal data protection while it is processed in the information systems as established by the Government of the Russian Federation;
- use of information security tools that have passed the conformity assessment procedure in order to phase out actual threats;
- implementation of the authorisation system for the employees' access to the personal data processed in the information systems and to hardware and software designed to protect the information;
- registration of and accounting for actions with the personal data taken by users of the information systems where the personal data is processed;
- registration of security events in the information system, the ability to view and analyse the information thereon and to respond thereto;
- identifying malicious software (using anti-virus programs) on all nodes of the Company's information network that have the respective technical capability;
- revealing invasions in the Company's information system that violate or predetermine a violation of the set requirements for securing the personal data;
- encrypting the personal data transferred via insecure communication channels, including the Internet, both when it is received from the counterparties in order to perform a contract and when it is sent to the counterparties;
- regular monitoring of user actions, investigations of violations of the personal data security requirements;
- revealing unauthorised violations of the integrity of the information system and the personal data contained therein, backup of the information for its recovery;
- recovering the personal data modified or destroyed as a result of unauthorised access thereto (creating a personal data backup and recovery system);
- preventing unauthorised access to the personal data processed in the virtual infrastructure;
- revealing, identifying and analysing incidents in the information system and taking measures to mitigate and prevent them;

- managing changes to the configuration of the information system and the personal data protection system, analysing the potential impact of scheduled changes on securing the personal data and documenting such changes;
- assessing the efficiency of personal data security measures;
- secure network interworking (firewalling);
- control over the compliance with these requirements (independently or with the involvement on a contractual basis of legal entities and individual entrepreneurs licensed for the technical protection of confidential information) at least once every 3 years.

11.10. The Company's information system must include a subsystem that ensures the personal data protection from unauthorised or accidental access thereto, destruction, modification, blocking, copying, sharing, dissemination thereof and from any other inappropriate actions in relation to the personal data.

11.11. When the information system is hosted in the data centre (cloud computing infrastructure), some of the security measures may be taken by the data centre (cloud computing provider) which is recorded in the contract between the Company and the data centre (provider).

11.12. The personal data security tools are installed and commissioned in the Company's information system in accordance with the operation, technical and project documentation.

11.13. The hosting of the personal data information systems, special equipment and supervision of the premises where the personal data is processed, the security regime in those premises must ensure the safety of the personal data media and the information security tools and to prevent uncontrolled entry into or stay in those premises of any intruders.

11.14. The entrance doors of the premises where the tangible media of the personal data are stored must be equipped with locks that ensure reliable closing of the premises during non-working hours.

11.15. To control the entrance, combination locks or other security tools may be installed; the premises are equipped with a burglar alarm, if required.

11.16. **Measures to Secure the Personal Data when Processed without Computer-Aided Facilities:**

11.16.1. When the personal data is processed without computer-aided facilities, it should be separated from any other information, in particular, by its recording on separate tangible media of personal data, such as forms of unified accounting for employees, etc.

11.16.2. When the personal data is recorded on the tangible media, it is not allowed to record on the same tangible medium any personal data the purposes of which processing are obviously incompatible with each other. When processing any personal data intended for various purposes, a separate tangible medium must be used for each such group of personal data.

11.16.3. The Company ensures separate storage of the personal data (tangible media) processed for various purposes.

11.16.4. The personal data processed without computer-aided facilities must be processed in such a way that enables to determine the places of storage of the personal data (tangible media) and to establish a list of persons processing the personal data or having access thereto, for each category of personal data. The documents containing the personal data (files with documents containing personal data of the employees, employment record books, file cabinets, accounting logs, books of record, questionnaires, etc.) must be kept at storage facilities that protect from unauthorised access. The places where the media of personal data processed without computer-aided facilities are stored are established by the list which form is in ***Appendix No. 15*** to the Policy.

11.16.5. The persons processing the personal data without computer-aided facilities must be informed:

- that they process the personal data processed without computer-aided facilities;
- on the categories and list of the personal data processed;
- on specific features and rules for such processing.

11.16.6. The informing of those persons is documented by the Company.

11.17. In case any computer incidents are revealed that result in the inappropriate transfer (sharing, dissemination, access) of the personal data, the Company informs the state system for revealing, preventing and mitigating computer attacks on information resources of the Russian Federation and interacts with such system in the manner prescribed by the federal executive authority authorised in the area of security.

11.18. In case any inappropriate or accidental transfer (sharing, dissemination, access) of the personal data is established that results in a violation of the personal data subjects' rights, the Company notifies the body authorised to protect the personal data subjects' rights from the moment such incident is revealed:

- of the incident, hypothetic causes that result in the violation of the personal data subjects' rights and hypothetic harm caused thereto, measures taken to mitigate the effects of the respective incident, and provides the information on the person authorised by the Company to interact with the body authorised to protect the personal data subjects' rights regarding issues related to the identified incident, within 24 hours;
- of results of the internal investigation of the incident revealed and provides the information on the persons whose actions caused the incident (if any), within 72 hours.

12. Final Provisions

12.1. The Policy is the Company by-law that enters into force from the time the Company manager signs the order to put it into effect and is valid until it is cancelled by order of

the Company manager and/or new regulations on the procedure for processing and securing the personal data are approved.

12.2. The current version of the Policy is available to any and all Website Users and Platform Users on the official website of the Company at https://www.ite.group/ and at the Platform addresses specified in this Policy. This Policy may be amended by the Company. Any amendments to the Policy are made by the Company independently and enter into force on the day following the day such amendments are published, unless otherwise specified in the Policy. The Website Users and Platform Users undertake to independently read the amendments made to the Policy. If the Website Users and the Platform Users use actually after amendments are made to the terms and conditions of this Policy this means that they accept the new terms and conditions.

12.3. All appendices specified in this Policy are an integral part hereof, but due to the fact that they do not apply to the Website Users and the Platform Users, they are not published at the Company's websites and the Platform.

12.4. Any other obligations and rights of the Company as the personal data controller and the person arranging for its processing on behalf of other controllers are determined by the personal data laws of the Russian Federation.

12.5. Any officers and Employees of the Company guilty of violating the rules governing the processing and protection of the personal data have financial, disciplinary, administrative, civil and criminal liability in accordance with the legislation of the Russian Federation.

12.6. Any legal entities that violate the contractual obligations to keep confidential the personal data and the general requirements for the personal data processing have civil and administrative liability in accordance with the legislation of the Russian Federation.

12.7. The provisions of the Policy are reviewed as often as required. The Policy is reviewed in a mandatory manner in case of material changes in the rules of international law binding upon Russia or the current personal data laws of the Russian Federation.

12.8. When the provisions of the Policy are amended, the following is taken into account:

- changes in the information infrastructure and/or the information technologies used by the Company;
- the practice of enforcement of the personal data laws in the Russian Federation;

changes in the conditions and specific features of the personal data processing by the Company due to the introduction of new information systems, processes and technologies into its business.