IP Kozhemyak Denis Vladimirovich

Rudneva ul, 21, corp 1, office 255., saint-petersburg, Russia, 194292

SEEN AND APPROVED

IP Kozhemyak D.V.

September 27, 2020
p/p

REGULATIONS ON PERSONAL DATA PROTECTION

St. Petersburg, 2020

I. GENERAL PROVISIONS

1.1 The purpose of these Regulations is to ensure protection of personal data of the employees, customers

and counterparts of the IP Kozhemyak Denis Vladimirovich, **PRSN:** 320784700107192
TIN: 780227462257, registered address: Rudneva ul, 21, corp 1, office 255., saint-petersburg, Russia, 194292(referred to hereinafter as “IP Kozhemyak d.v.” LCC) against unauthorized access, inappropriate use, or loss.

1.2 These Regulations have been elaborated in compliance with the Russian Federation Constitution, the Federal Law No. 152-ФЗ dd. July 25, 2006 “On Personal Data”, the Federal Law No. 149- ФЗ dd. July 27, 2006 “On Informatization, Informaton Technologies and Protection of Information”, Decrees of the Russian Federation Government No. 1119 dd. November 01, 2012 “On Approval of Requirements to Personal Data Protection in the Course of Procession thereof within the Personal Data Information Systems”, and No. 687 dd. September 15, 2008 “On Approval of Regulations on Peculiarities of Personal Data Processing carried out Without the Use of Means of Automation”, as well as in compliance with other regulatory acts in force in the territory of the Russian Federation.

1.3 The following terms and definitions are used in these Regulations:
Operator – IP Kozhemyak d.v. LLC, that has entered into contractual relations with an employee, a customer or a counterpart, or provides services to an individual, a legal entity or an individual entrepreneur.
Customer – an individual, a legal entity represented by an authorized representative, an individual entrepreneur or an authorized representative thereof, related to microfinance who has entered into contractual relations with the Company.
Counterpart – an individual, a legal entity represented by an authorized representative, an individual entrepreneur or an authorized representative thereof who has entered into contractual relations with the Company in relation to economic activities.
Personal data of the Customer - information required by the Operator in connection with the contractual relations and referring to a particular Customer, including his/her name, given name, patronymic, year, month, date and place of birth, address, marital status, education, profession, qualification, occupation, position, income, e-mail address, telephone number, and other information specified by the applicant.
Personal data of the Counterpart - information required by the Operator in connection with contractual relations and referring to a particular Counterpart, including name, given name, patronymic, year, month, date and place of birth, address, passport data, e-mail address, telephone number, tax status (resident/non-resident), other information specified by the applicant.
Personal data of the Employee - information required by the Company as an employer in connection with employment relations and referring to a specific employee. Information on facts, events and life circumstances of employee which allow to identify the employee’s personality is understood as such personal data, including:
-name, given name, patronymic;
-education;
-information on work and general experience;
-information on the family composition;
-passport data;
-information on the employee's salary;
-qualification;
-position held;
- address of place of residence;
-phone number;

Personal data processing - any action (operation) or set of actions (operations) undertaken with use of means of automation or without use of such means in respect of the personal data, including gathering, recording, systematization, accumulation, storage, validation (updating, change), extraction, use, transfer (distribution, submission, access), depersonalization, blocking, removal, destruction of the personal data.
Personal data subject – Employee, Customer, Counterpart.
Protection of Personal Data of the Employee/Customer/Counterpart - the Company's activities to ensure the confidentiality of information through the local regulation of personal data processing and organizational and technical measures.

Confidentiality of the personal data - requirement not to allow distribution of such data without the consent of the subject of the personal data or in the absence of other legal basis, the observance of which is obligatory for the person who has obtained access to the personal data.
IS (Information Security) Division - an employee of the Company responsible for ensuring information security and for the compliance with the procedures of IP Kozhemyak d.v. LLC, including the responsibility for arrangement of the personal data processing.
HR department – an employee of IP Kozhemyak d.v. LLC is responsible for working with the personnel (human resources) of the IP Kozhemyak d.v. LLC.
Personal Data Information System (PDIS) - a set of personal data contained in databases and ensuring processing thereof via information technologies and technical means.

1.4 Personal data of the Company's employees are classified as confidential information. Non-disclosure requirements shall be neglected in cases of depersonalization or upon the elapse of 20 years of storage, unless otherwise provided by the legislation of the Russian Federation.

1.5. The period of storage of personal data of customers and counterparts comprises 5 years from the date of termination of civil law relations, provided that the customer (counterpart) has not filed a notice of termination of consent to process his/her personal data within the specified period.

1.6. These Regulations apply to all Employees, Customers and Counterparts.

II. PERSONAL DATA PROCESSING

2.1 In order to secure human and citizen's rights and freedoms, the Company and/or its representatives shall observe the following general requirements when processing personal data:
2.1.1 Processing of personal data shall be carried out on legal and fair basis, solely for the purpose of ensuring compliance with laws and other regulatory legal acts, assistance in fulfillment of contractual obligations under the legislation of the Russian Federation;

2.1.2 Personal data processing shall be limited to the achievement of specific, predetermined and legitimate goals. Processing that is incompatible with the purposes of collecting personal data shall not be allowed.

2.1.3 The Company's obtaining of personal data may be carried out either by submitting such data by the employee, customer, counterpart, or by obtaining such data from other sources.

2.1.4 Personal data shall be obtained by the Company directly from the employee, customer or counterpart. If the employee's personal data can only be obtained from a third party, the subject of personal data must be notified of it in advance, and a written consent must be obtained from the personal data subject. The Company shall inform the subject of personal data of the purposes, intended sources and methods of obtaining personal data, as well as the nature of the personal data subject to obtaining and the consequences of refusal to give a written consent to receive such data.

2.1.5. The Company shall have no right to receive and process personal data of an employee, customer, counterpart concerning his/her political, religious and other beliefs and private life. In cases directly related to the issues of labor relations, data on the private life of the employee, customer, counterparty (information on life activities in the sphere of family life, personal relationships) can be obtained and processed by the Company only with the written consent from the employee/customer/counterpart.

2.1.6. The Company shall have no right to receive and process personal data of an employee, customer or counterpart on his/her membership in public associations or his/her trade union activities, except for the cases stipulated by the Federal Laws.

2.2. Personal data may be processed, transferred and stored by, or when:
□ Director General of the Company;
□ Heads of structural units by business area (access to personal data only in regard of employees of such structural units);
□ when transferring from one structural unit to another, the head of a new unit may have access to

personal data of the employee;
□ employee, as data source;
□ other employees of the organization when performing their official duties.

2.3. The personal data processing shall only be possible in accordance with the purposes that determined the receipt thereof. Personal data may not be used for the purposes of inflicting property and moral harm to citizens or for preventing the citizens of the Russian Federation to exercise their rights and freedoms. Restriction of the rights of citizens of the Russian Federation on the basis of the use of information on their social origin and on racial, national, language, religious and party affiliation is prohibited by the current legislation of the Russian Federation.

2.4. In making decisions affecting the interests of the customer or counterpart, the Operator shall have no right to act on the basis of personal data of such customer or counterpart obtained solely as a result of automated processing thereof without a written consent to such actions from the customer or counterpart.

2.5. When identifying a customer or a counterpart, the Company may request to submit identity documents and documents confirming the authority of the representative.

2.6. Upon conclusion of the contract, as well as in the course of contract performance, it may be necessary for the customer of the counterpart to provide other documents containing information about the customer or counterpart.

2.7. After the decision to conclude the contract or after submission of documents confirming the authority of the representative, as well as subsequently, in the process of execution of the contract, the following shall be regarded as the documents containing personal data of the customer or counterpart:
- contracts;
- orders on principal activities;
- service memoranda;
- admission orders for the of representatives of the customer or counterpart;
- one-time or temporary passes;
- other documents, the inclusion of personal data of the customer or counterpart into which is necessary in accordance with current legislation.

2.8. 2.8. Transfer of personal data shall only be possible with the consent of the employee, customer, counterpart, or in cases directly provided for by the legislation of the Russian Federation.
2.8.1. The Company shall observe the following requirements when transferring personal data:
□ Not to disclose personal data to any third party without the written consent of the employee, customer, counterpart, except for the cases when such transfer is necessary to prevent a threat to the life and health of the employee, customer, counterpart, as well as in cases stipulated by the legislation of the Russian Federation;
□ Not to disclose personal data for commercial purposes without the written consent of the data subject;
□ To warn the individuals and entities receiving personal data that such data can only be used for the purposes for which they are reported and require from such individuals and entities a confirmation that this rule is observed. Individuals and entities receiving personal data are obliged to observe secrecy (confidentiality). This provision does not apply to the exchange of personal data in the manner prescribed by the legislation of the Russian Federation;
□ To allow access to personal data only for specially authorized persons identified by order of the Company's Director, and with this, such persons shall have the right to receive only such personal data that are required to perform specific functions;
□ Not to request information on health status of the employee, except for the data that are related to the possibility of the employee to perform labor function;
□ To provide employee's personal data to employees' representatives as required by the Labor Code and limit this information to only such personal data of the employee that are required for these representatives to perform their functions.
2.8.2 Transfer of personal data from the Company and (or) its representatives to the external user may be allowed in the minimum amount and only for the purpose of performing tasks corresponding to the objective cause of collecting such data.

2.8.3. When transferring personal data to external users (including such transfer for commercial purposes) the Company shall not communicate such data to the third party without a written consent of the employee, the customer, the counterpart, except for the cases stipulated by the legislation of the Russian Federation.

2.9. All confidentiality precautions in the course of collection, processing and storage of personal data shall apply to both hard and soft (automated) media.

2.10. It is not allowed to answer questions related to the transfer of personal data by phone or fax.

2.11. Storage of personal data shall be carried out in a manner excluding a possibility of loss or inappropriate use thereof.

2.12. The period of storage and processing of personal data shall be determined in accordance with the Law "On Personal Data". Processing of personal data starts from the moment when such personal data have been entered into information systems of personal data, and shall stop:
- In case of revealing of illegal actions with the personal data within the time not exceeding three working days from the date of such revealing. The Company shall eliminate the detected infringements. If elimination of infringements is impossible, the Company shall delete the personal data within a period not exceeding three working days from the date of detection of illegal actions with personal data.
The Company shall notify the subject of the personal data or the legal representative of the subject on elimination of the infringements or on destruction of the personal data, and in case an application or inquiry has been directed by an authorized body on protection of the rights of subjects of the personal data, the Company shall also notify such authorized body;
- If the purpose of personal data processing has been achieved, the Company shall immediately cease processing of the personal data and destroy the relevant personal data within a period not exceeding three working days from the date of having achieved the purpose of personal data processing, and shall notify the subject of personal data or the legal representative thereof, and an application or inquiry has been directed by an authorized body for the protection of the rights of subjects of personal data, the Company shall also notify the said body;
- in case of withdrawal of the consent to process personal data by the subject of personal data, the Company shall terminate the processing of personal data and delete personal data within a period not exceeding three working days from the date of receipt of such withdrawal. The Company shall notify the subject of personal data about the destruction of personal data.
In case of the Company's winding up.

2.13. Unless otherwise provided by the federal law the Operator shall have the right to entrust processing of the personal data to another person/entity with the consent of the subject of the personal data, on the basis of a contract concluded with this person/entity, including the state or municipal contract, or by means of acceptance of a corresponding statement by the state or municipal body (further - the Operator's instruction). The person/entity charged with the processing of the personal data under the Operator's instruction shall be obliged to observe principles and rules of processing of the personal data provided by the Federal Law No. 152-ФЗ dd. July 27, 2006 "On Personal Data". The Operator's instruction shall contain the list of actions (operations) with the personal data to be made by the person/entity charged with processing of the personal data, and the purposes of processing, the duty of such person/entity to observe confidentiality of the personal data and to ensure safety of the personal data during processing shall be established, and also the requirements to protection of the processed personal data according to article 19 of the Federal Law No. 152-ФЗ dd. July 27, 2006 "On Personal Data" shall be specified.

2.14. The person/entity charged with the processing of the personal data under the Operator's instruction is not obliged to receive the consent of the subject of the personal data to process such personal data.

2.15. In case that the Operator entrusts processing of the personal data to another person/entity, the Operator shall be liable before the subject of the personal data for actions of the specified person/entity. The person/entity charged with processing of the personal data under the Operator's instruction shall be liable before the Operator.

III. ACCESS TO PERSONAL DATA

3.1. The list of the persons authorized to process the personal data ("the List") and liable according to the legislation of the Russian Federation for infringement of rules of the personal data processing shall be defined and confirmed by the Director.

3.2. At the moment of hiring, dismissal or change of job duties of Employees, the HR department shall make changes in the list of the persons authorized to process the personal data not later than in three days, in coordination with the IS division.

3.3. The IS division shall, at least once a quarter, check the List for relevance. In case of revealing any discrepancies, the HR department shall introduce changes to the List.

3.4. The Employees of the Company shall process the personal data in accordance with the functions assigned to such Employees.

3.5 Access to personal data shall be granted only to the persons occupying positions on the List. Granting access to PDIS shall be carried out in accordance with the Instruction on the Procedure for Admission of to PDIS Information Resources and the Premises of the Company's Informatization Unit.

3.6. The Employees shall have permission to enter and correct personal data within the limits defined by their job duties.

3.7. Individuals/entities granted access to personal data shall keep confidential any information known to them and inform the IS division about leakage of personal data, facts of violation of the order of personal data processing, attempts of unauthorized access to personal data.

3.8 The individuals/entities granted access to personal data shall use the data only for the purposes for which such personal data have been submitted, and are obliged to observe the confidentiality and make a commitment of personal data non-disclosure.

IV. PERSONAL DATA PROTECTION

4.1 All employees who have access to personal data must sign a non-disclosure agreement.
4.2. Protection of the personal data from inappropriate use or loss shall be provided by the Operator in an order established by the legislation of the Russian Federation.
4.3. Employees, customers or counterparts shall have a possibility to familiarize themselves with these Regulations before submitting their personal data.
4.4. The following information is subject to protection:
- information about personal data of the subject;
- documents containing personal data of the subject;
- personal data contained in electronic media.

4.5 The Operator shall appoint a person responsible for arrangement of the personal data processing.
4.6. The Operator shall issue the documents defining a policy of the Operator concerning processing of the personal data, local acts concerning processing of the personal data, and also the local acts establishing the procedures directed at prevention and detection of infringements of the Russian Federation legislation and elimination of consequences of such infringements.
4.7. The Operator shall take necessary legal, organizational and technical measures or ensure taking such measures for protection of the personal data against illegal or accidental access to such data, destruction of such data, changes, blocking, copying, granting, distribution of the personal data, and/or other illegal actions in respect of the personal data according to article 19 of the Federal Law No. 152-ФЗ dd. July 27, 2006 "On Personal Data", including:
1) identification of threats to safety of the personal data in the course of processing via personal data information systems;
2) implementation of organizational and technical measures for safety of the personal data in the course of processing via personal data information systems necessary for fulfillment of requirements towards protection of the personal data which guarantees levels of the personal data safety established by the Government of the Russian Federation;
3) application of the means of information protection which have passed the approved procedure of conformity assessment ;

4) efficiency assessment of adopted personal data safety measures before commissioning of the personal data information system;
5) registration of the personal data media;
6) detection of facts of unauthorized access to personal data and taking corrective measures;
7) restoration of the personal data modified or destroyed as a result of unauthorized access;
8) establishment of rules of access to personal data processed in the personal data information system as well as ensuring registration and accounting of all actions performed with personal data in the personal data information system;
9) control over measures taken to ensure the security of personal data and the level of security of personal data information systems.
4.9. The Operator shall carry out internal control and/or audit of compliance of personal data processing with the Federal Law No. 152-ФЗ dd. July 27, 2006 "On Personal Data" and regulatory legal acts adopted in accordance therewith, requirements for the protection of personal data, Operator policy regarding the processing of personal data, local acts of the Operator.
4.10. The Operator shall estimate the damage which can be caused to subjects of the personal data in case of infringement of the said Federal Law, a parity of the said damage and the measures taken by the Operator directed at maintenance of performance of the duties set forth by the said Federal Law;
4.10. The Operator shall arrange for familiarization of its Employees directly engaged in personal data processing with provisions of the legislation of the Russian Federation on personal data, including requirements to protection of the personal data, the documents defining a policy of the Operator concerning processing of the personal data, local acts concerning processing of the personal data, and (or) training of the specified Employees;
4.11. Responsible persons of the corresponding divisions storing personal data in hard and soft media shall ensure protection of such data against unauthorized access and copying according to the "Regulation on peculiarities of personal data processing carried out without the use of automation means" approved by the Decree of the Russian Federation Government No. 687 dd. September 15, 2008 “On Approval of Regulations on Peculiarities of Personal Data Processing carried out Without the Use of Means of Automation”.
4.12. The responsible persons of the structural divisions processing the personal data in the personal data information systems and data media shall ensure protection according to the Decree of the Russian Federation Government No. 687 dd. September 15, 2008 “On Approval of Regulations on Peculiarities of Personal Data Processing carried out Without the Use of Means of Automation” and other normative, methodological documents, and guidelines.
4.13. Whenever possible, the personal data shall be depersonalized.
4.14. Threats analysis.
Safety of the personal data, and elaboration and introduction of means of the personal data protection are based on the analysis of threats to safety of the personal data.
The Company, if necessary, shall develop and support Particular Model of threats to safety of the personal data in course of processing via the personal data information systems (“ Particular Model of Threats”).
The Particular Model of Threats reflects an actual state of safety of the personal data information systems and actual threats to safety of the personal data. Elaboration of the Particular Model of Threats is carried out on the basis of the analysis of existing threats to safety and possibility of implementation thereof in the personal data information systems under survey.
4.15. Procedure of personal data destruction.
A person responsible for destruction of personal data is the one authorized and appointed by order of the Director General.
The authorized person is the Chairman of the Company's committee for destruction of personal data. Appointment of the committee for destruction of personal data is made by order of the Director General.
Upon the occurrence of any event that according to the legislation of the Russian Federation entailed the need to destroy personal data, the Authorized person shall:
- Notify the members of the committee for destruction of personal data;
- Determine (appoint) the time and place of work of the committee (time and place of destruction of personal data);
- Establish a list, type, name, registration numbers and other information of data media on which personal data subject to destruction are stored (and/or tangible data media);
- Determine the technology (method, procedure) of personal data destruction (and/or tangible personal

data media);
- Determine the technical (material, software and other) means by which the destruction of personal data will be carried out;
- Destroy personal data by managing the work of the committee members (and / or tangible personal data media);
- Prepare an appropriate Act on destruction of personal data (and/or tangible personal data media) and submit the Act on destruction of personal data (and/or tangible personal data media) for approval by the Director;
- If necessary, notify the personal data subject and/or the authorized body about the destruction of the personal data.

V.RIGHTS AND OBLIGATIONS OF THE EMPLOYEE

5.1 Employees and their representatives shall be familiarized with the Company's documents establishing the procedure for processing personal data of employees, as well as their rights and obligations in this area, against signed receipt.
5.2 In order to protect personal data held by the employer, the employee shall have the right to:
□ demand exclusion or correction of incorrect or incomplete personal data;
□ freely access his/her personal data, including the right to receive copies of any record containing personal data;
□ supplement personal data of evaluative nature with a statement expressing his/her own viewpoint;
□ identify his/her representatives to protect his/her personal data;
□ preserve and protect his/her personal and family secrets.
5.3. The Employee is obliged to:
□ submit to the Company and/or his/her representative a set of reliable, documented personal data, the composition of which is established by the Labor Code of the Russian Federation.
□ report to the Company on changes in his/her personal data in a timely manner.
5.4 The Employees shall notify the Company of any changes in their name, given name, patronymic, date of birth, which is reflected in the employment record book based on the submitted documents. If necessary, the data on education, profession, specialty, assigning a new grade, etc. shall also be changed.
5.5. In order to protect private life, personal and family secrets, the employees shall have the right to refuse to process personal data without their consent.

VI.RIGHTS AND OBLIGATIONS OF THE CUSTOMERS AND COUNTERPARTS

6.1. In order to ensure protection of personal data stored with the Operator, the customers and counterparts are entitled to:
6.1.1 Obtain complete information about the composition of personal data and processing thereof, in particular, the customer or counterpart has the right to know who uses or has used information about such personal data, and for what purposes.
6.1.2. Access personal data freely, including the right to receive copies of any record containing personal data of the customer or counterpart, except as provided by the legislation of the Russian Federation.
6.1.3. Appoint their representatives to protect the personal data.
6.1.4. Require to exclude or correct incorrect or incomplete, outdated, unreliable, illegally obtained personal data or personal data unnecessary for the Operator. In case that the Operator refuses to exclude or correct the personal data of the customer or the counterpart, such customer or counterpart shall have the right to declare to the Operator in writing about its disagreement and give corresponding substantiation of such disagreement.
6.1.5. Require the Operator to notify all persons who have previously been informed of incorrect or incomplete personal data of the customer or counterpart, of all exceptions, corrections or additions made thereto.
6.1.6. Make judicial appeal against any illegal actions or omissions of the Operator in processing and protection of personal data of the customer/counterpart.
6.2. In order to ensure the accuracy of personal data, the customer and the counterpart are obliged to:
6.2.1 Provide the Operator with complete and reliable data at the moment of conclusion of the contract;
6.2.2 In case of change of the information constituting personal data of the customer or counterpart, submit this information to the Operator immediately but not later than within five working days.

VII.LIABILITY FOR DISCLOSURE OF CONFIDENTIAL INFORMATION RELATED TO

PERSONAL DATA OF THE EMPLOYEES

7.1. Legal entities and individuals holding information about citizens, receiving and using it in accordance with their powers, shall be liable in accordance with the laws of the Russian Federation for violation of the protection, processing and use of such information.
7.2 The manager authorizing access to a confidential document shall be held personally liable for such authorization.
7.3 Each employee of the organization receiving a confidential document for work shall be held personally liable for safety of the medium and confidentiality of the information.
7.4. Individuals and entities found guilty of violation of norms regulating receipt, processing and protection of personal data shall bear disciplinary, administrative, civil or criminal liability according to the legislation of the Russian Federation.
7.4.1. The Company shall have the right to impose disciplinary sanctions provided for by the Labor Code of the Russian Federation in case of the employee's failure to perform, or improper performance, through his or her fault, of his or her duties to comply with the established procedure for handling confidential information.
7.4.2. Officers whose duties include processing personal data shall provide everyone with an opportunity to familiarize themselves with documents and materials directly affecting their rights and freedoms, unless otherwise provided by law. Unjustified refusal to provide documents collected in accordance with the established procedure, or untimely provision of such documents or other information in cases stipulated by law, or provision of incomplete or knowingly false information shall result in imposing an administrative penalty on officers in the amount determined by the Code on Administrative Offences.
7.4.3 In accordance with the Civil Code, individuals/entities who have illegally obtained information constituting official secrets are obliged to reimburse the caused losses, and the same obligation shall be imposed on the employees.
7.4.4. Criminal liability for violation of inviolability personal privacy (including illegal collection or dissemination of information on private life of a person constituting his/her personal or family secret without his/her consent), illegal access to computer information protected by law, illegal refusal to provide documents and information collected in accordance with the established procedure (if these actions have caused damage to rights and legitimate interests of citizens) committed by a person using his/her official position shall be punished by a fine, or deprivation of the right to hold certain posts or engage in certain activities, or arrest.
7.5. Illegal actions of public authorities and organizations for collection and use of personal data can be established judicially.

VIII.RESPONSIBILITY OF THE EMPLOYEES TO OBSERVE CONFIDENTIALITY OF PERSONAL DATA

8.1. In order to ensure the confidentiality of information, all employees shall:
8.1.1 Not disclose information constituting trade secret of the Company, except for cases when a written consent of the head of the Company has been given to do so.
8.1.2. Not use the information constituting the trade secret of the Company for other activities, in the course of work for another organization, enterprise, institution, by order of an individual or in the course of conducting business, as well as for personal purposes.
8.1.3.Comply with the commercial secrecy provisions established by the Company.
8.1.4. Immediately inform the direct superior and the head of the Company of the need to answer or of having answered the questions regarding the Company's trade secrets of the officials of the competent authorities (tax inspection, preliminary investigation bodies, etc.) on duty.
8.1.5. Immediately inform the direct superior and the head of the Company of the loss or shortage of trade secret information media, certificates, passes, room keys, vaults, safes, personal seals and other facts that may lead to the disclosure of trade secret of the Company, as well as the causes and conditions of possible leakage of trade secret information.
8.1.6 Immediately notify the direct superior and the head of the Company in the event of an attempt to obtain information from an employee that contains a trade secret of the Company by unauthorized persons.
8.1.7. Not create conditions for the leakage of information constituting a trade secret and make every effort to stop such leakage if the employee becomes aware that a leakage is taking place or that conditions for the possibility of such leakage exist.
8.1.8. Not disclose or use trade secrets on his/her own behalf or on behalf of other persons within five

years after termination of the employment contract with the Company (regardless of the reasons for dismissal).
8.1.9. Upon termination of the employment contract or civil law contract, transfer tangible data media available to the employee with information constituting trade secret to the Company.

IX.FINAL PROVISIONS

9.1 These Regulations shall come into force upon being approved by order of the Director.
9.2 These Regulations shall be communicated to all Company's employees personally against signed receipt.