INDIVIDUAL ENTREPRENEUR CHACHINA IRINA GENNADIEVNA INN: 774361298675,
OGRN: 322774600034231 125475 Russia
MOSCOW, ST. DYBENKO, D 6, Bldg. 1, KV 353

POSITION
ABOUT PROTECTION OF PERSONAL DATA

Moscow

2023

I. GENERAL PROVISIONS The purpose of these Regulations is to protect the personal data of employees, clients and contractors of the individual entrepreneur Chachina Irina Gennadievna inn: 774361298675, urn: 322774600034231. index: 125475 Russia, Moscow, st. Dybenko, 6, building 1, apartment 353 (hereinafter referred to as IP Chachina Irina Gennadievna), from unauthorized access, unlawful use or loss. 1.1. These Regulations have been developed in accordance with the Constitution of the Russian Federation, Federal Law No. 152-FZ dated July 27, 2006 “On Personal Data”, Federal Law No. 115-FZ, Federal Law No. 149-FZ dated July 27, 2006 “On Informatization, Information Technologies and on the protection of information”, Resolutions of the Government of the Russian Federation dated November 1, 2012 No. 1119 “On approval of requirements for the protection of personal data during their processing in personal data information systems” and dated September 15, 2008 No. 687 “On approval of the Regulations on the specifics of processing personal data, carried out without the use of automation tools”, other regulations in force on the territory of the Russian Federation. 1.2. The following terms and definitions are used in these Regulations: Operator – individual entrepreneur Irina Gennadievna Chachina, who has entered into a contractual relationship with an employee, client or counterparty, or provides services to an individual, legal entity or individual entrepreneur. Client - an individual, a legal entity represented by an authorized representative, an individual entrepreneur or his authorized representative who has entered into a contractual relationship with the company related to microfinance. Counterparty is an individual, a legal entity represented by an authorized representative, an individual entrepreneur or his authorized representative who has entered into a contractual relationship with the company on issues of economic activity. Personal data of the Client - information required by the Operator in connection with contractual relations and relating to a specific Client, including his last name, first name, patronymic, year, month, date and place of birth, address, marital status, education, profession, specialty, position held , income, email address, phone number, other information specified by the applicant. Personal data of the Counterparty - information required by the Operator in connection with contractual relations and relating to a specific Counterparty, including last name, first name, patronymic, year, month, date and place of birth, address, passport details, email address, telephone, 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 labor relations and relating to a specific employee. Information about employees means information about facts, events and circumstances of an employee’s life that allow his or her identity to be identified, including: - last name, first name, patronymic; - education; - information about labor and general experience;

- information about family composition;
- passport data; - information about the employee’s salary; - speciality; - position held; - residence address; - telephone;

Processing of personal data – any action (operation) or set of actions (operations) performed using automation tools or without the use of such means with personal data, including collection, recording, systematization, accumulation, storage, clarification (updating, changing), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of personal data. Subject of personal data – Employee, Client, Counterparty. Protection of personal data of an Employee, Client, Counterparty - the Company's activities to ensure, through local regulation, the procedure for processing personal data and organizational and technical measures of information confidentiality.
Confidentiality of personal data is a mandatory requirement for a person who has
access to personal data to not allow their distribution without the consent of the subject of personal data or the presence of another legal basis. The IS division is an employee of the Company who is entrusted with responsibilities for ensuring information security and the regime of the individual entrepreneur "Irina Gennadievna Chachina", including
responsibilities for organizing the processing of personal data. The personnel department is an employee of the IP "Chachina Irina Gennadievna", who is entrusted with the responsibilities for working with the personnel of the IP "Chachina Irina Gennadievna". Personal data information system (ISPDn) is a set of personal data contained in databases and
information technologies that ensure their processing and technical means. 1.3. Personal data of the Company's employees is classified as confidential information. The confidentiality regime of personal data is lifted in cases of depersonalization or after the expiration of 20 years of storage period, unless otherwise determined by the
legislation of the Russian Federation. 1.4. The storage period for personal data of clients and counterparties is 5 years from the date of termination of civil law relations, provided that the client (counterparty) has not received a notification of withdrawal of consent to the processing of personal data within the specified period. 1.5. These Regulations apply to all Employees, Clients and Counterparties.

II. PROCESSING OF PERSONAL DATA

2.1. In order to ensure the rights and freedoms of humans and citizens, the company and (or) its representatives when processing personal data must comply with the following general requirements: 2.1.1. The
processing of personal data must be carried out on a legal and fair basis, solely for the purpose of ensuring compliance with laws and other regulations, facilitating the fulfillment of contractual obligations in accordance with the legislation of the Russian Federation; 2.1.2. The processing of personal data must be limited to the achievement of specific,
pre-defined and legitimate purposes. Processing of personal data that is incompatible with the purposes of collecting personal data is not permitted. 2.1.3. The company can obtain personal data either by submitting it to the employee, client, or counterparty themselves, or by
receiving it from other

sources.

2.1.4. Personal data is obtained by the company directly from the employee, client, or counterparty. If the employee's personal data can only be obtained from a third party, then the subject of the personal data must be notified about this in advance, and written consent must be obtained from him. The company must inform the subject of personal data about the purposes, intended sources and methods of obtaining personal data.

data, as well as the nature of the personal data to be received and the consequences of refusal to give written consent to receive it. 2.1.5. the company does not have the right to receive and process
personal data of an employee, client, contractor about his political, religious and other beliefs and private life. In cases directly related to issues of labor relations, data about the private life of an employee, client, contractor (information about life activities in the field of family, household, personal relationships) can be received and processed by the company only from his written

consent.

2.1.6. the company does not have the right to receive and process personal data of an employee, client, contractor about his membership in public associations or his trade union activities, except in cases provided for by federal laws. 2.2. The following may have access to the processing, transfer and storage of personal data: Chachina Irina Gennadievna; Heads of
structural divisions in the area of activity (access to personal data only of employees of their department);
-
-

- when transferring from one structural unit to another, access to personal
The employee's data may be available to the head of the new unit; the employee himself, the
- source of the data; other employees of the
- organization in the performance of their official duties. 2.3. The use of personal data is possible only in accordance with the purposes that determined its receipt. Personal data cannot be used to cause property and moral harm to citizens, or to impede the exercise of the rights and freedoms of citizens of the Russian Federation. Restriction of the rights of citizens of the Russian Federation based on the use of information about their social origin, racial, national, linguistic, religious and party affiliation is prohibited by the current legislation of the Russian Federation. 2.4. When making decisions affecting the interests of a client or counterparty, the Operator has no right to rely on the personal data of the client or counterparty obtained solely as a result of their automated processing without his written consent to such actions. 2.5. When identifying a client or counterparty, Individual Entrepreneur "Chachina Irina Gennadievna" may request
the presentation of identification documents and confirming the authority of the representative. 2.6. When concluding an agreement, as well as during the execution of an agreement, it may be necessary for the client or counterparty to provide other documents containing information about it. 2.7. After making a decision to conclude an agreement or submitting documents confirming the authority of the
representative, as well as subsequently, in the process of executing an agreement containing personal data of the client or counterparty, the following will also apply: - agreements; - orders for core activities; - office notes; - orders for the admission of representatives of the client,
counterparty; - one-time or temporary passes; - other documents where the inclusion of personal data of the client or counterparty is necessary in accordance with current legislation. 2.8. Transfer of personal data is possible only with the consent of the employee, client, counterparty or in
cases directly provided for by the legislation of the Russian Federation. 2.8.1. When transferring personal data, the company must comply with the following requirements: do not disclose personal data to a third party without the written consent of the employee, client, counterparty, except in cases where this is necessary in order to prevent a threat to the life and health of the employee, client, counterparty,
as well as in cases established legislation of the
Russian Federation;

-

 do not disclose personal data for commercial purposes without his written consent; warn persons receiving personal
 data that this data can only be used for the purposes for which they are communicated, and require these persons to confirm that this rule is observed. Persons receiving personal data are required to observe a regime of secrecy (confidentiality). This provision does not apply to the exchange of personal data in the manner established by the legislation of the Russian Federation; allow access to personal data only to specially authorized persons identified by Irina Gennadievna Chachina, while these persons should have the right to receive only those personal data that are necessary to perform specific functions; do not request
 information about the employee's health status, except for the information

 which relate to the issue of the employee's ability to perform a labor function; transfer the employee's personal data to
 employee representatives in the manner prescribed by the Labor Code, and limit this information only to those employee personal data that are necessary for the said representatives to perform their functions. 2.8.2. The transfer of personal data from the individual entrepreneur "Chachina Irina Gennadievna" and (or) its representatives to external consumers may be allowed in minimal amounts and only
for the purpose of performing tasks that correspond to the objective reason for collecting this data. 2.8.3. When transferring personal data to external consumers (including for commercial purposes), the company must not disclose this data to a third party without the written consent of the employee, client, or counterparty, except in cases established by the legislation of the Russian Federation. 2.9. All confidentiality measures in the collection, processing and storage of personal data apply to both paper and electronic (automated) media. 2.10. It is not allowed to answer questions related to the transfer of personal information by telephone or fax. 2.11. Personal data must be stored in a manner that prevents its loss or misuse. 2.12. The period of storage and processing of personal data is
determined in accordance with the Law "On Personal Data". The processing of personal data begins from the moment personal data is received in the personal data information systems and ends: - in case of detection of illegal actions with personal data within a period not
exceeding three working days from the date of such detection, the company eliminates the violations. If it is impossible to eliminate the violations committed,
the company destroys the personal data within a period not exceeding three working days from the date of discovery of illegal actions with personal data. The company notifies
the subject of personal data or his legal representative about the elimination of violations or the destruction of personal data, and if the appeal or request was sent by the authorized body for the protection of the rights of personal data subjects, the company also notifies the specified body; - if the purpose of processing personal data is achieved, the company immediately stops
processing personal data and destroys the corresponding personal data within a period not exceeding three working days
from the date of achieving the purpose of processing personal data, and notifies the subject of personal data or his legal representative about this, and in the event , if the appeal or request was sent by the authorized body for the protection of the rights of personal data subjects, the company also notifies the specified body; - if the subject of personal data withdraws consent to the processing of his personal data, the company stops
processing personal data and destroys personal data

data within a period not exceeding three working days from the date of receipt of the specified review. The company notifies the subject of personal data about the destruction of personal data. - in case of termination of the Company's activities. 2.13.
The operator has the right to entrust the processing of personal
data to another person with the consent of the subject of personal data, unless otherwise provided by federal law, on the basis of an agreement concluded with this person, including a state or municipal contract, or by adoption of a corresponding act by a state or municipal body (hereinafter referred to as the assignment operator). The person processing personal data on behalf of the operator is obliged to comply with the principles and rules for processing personal data provided for by Federal Law No. 152-FZ of July 27, 2006 "On Personal Data". The operator's instructions must define a list of actions (operations) with personal data that will be performed by the person processing personal data and the purposes of processing, the obligation of such a person must be established to maintain the confidentiality of personal data and ensure the security of personal data during their processing, as well as requirements for the protection of processed personal data must be specified in accordance with Article 19 of the Federal Law of July 27, 2006 No. 152-FZ "On Personal

data."
2.14. A person processing personal data on behalf of an operator is not required to obtain the consent of the subject of personal data to process his personal data.
data.
2.15. If the operator entrusts the processing of personal data to another person, the operator is responsible to the subject of personal data for the actions of the specified person. The person processing personal data on behalf of the operator is responsible to the operator.

III. ACCESS TO PERSONAL DATA

3.1. The list of persons authorized to process personal data (hereinafter referred to as the List) and who are responsible in accordance with the legislation of the Russian Federation for violation of the rules for processing personal data is determined and approved by the director. 3.2. When hiring, dismissing or changing the job responsibilities of Employees, the
Human Resources Division, no later than three days, makes changes to the list of persons authorized to process personal data, in agreement with the Information Security Division. 3.3. The information security department is required to check the relevance of the List at least once a quarter. If discrepancies are identified, the Human Resources Division makes changes to the List. 3.4.

Employees of IP "Chachina Irina Gennadievna" perform actions to process personal data in accordance with the functions assigned to employees. 3.5. Access to personal data is provided only to persons filling positions on the List. Providing access to ISPD is carried out
in accordance with the "Instructions on the procedure for admitting persons to information resources of ISPD and to the premises of the informatization facility of IP "Chachina Irina Gennadievna". 3.6. Employees have access to enter and
correct personal data within the limits determined by their job responsibilities. 3.7. Persons who have access to personal data must keep confidential information of a confidential nature known to them and inform the Information Security Division about the leak of personal data, violations of the procedure for handling them, and attempts of unauthorized access to personal data.

3.8. Persons who have access to personal data must use this data only for the purposes for which they were communicated, are obliged to maintain confidentiality and undertake an obligation of non-disclosure of personal data.

IV. PROTECTION OF PERSONAL INFORMATION

4.1. All employees who have access to personal data are required to sign a non-disclosure agreement. 4.2. Protection of personal data from unlawful use or loss is ensured by the Operator in the
manner established by the legislation of the Russian Federation. 4.3. Employees, clients or contractors must have the opportunity to familiarize themselves with this Regulation before providing their personal data. 4.4. The following are subject to
protection: - information about the subject's personal data; - documents containing personal data of the subject; - personal data contained on electronic media. 4.5. The operator appoints someone responsible for organizing the
processing of personal data.

4.6. The operator issues documents defining the operator's policy
regarding the processing of personal data, local acts on the processing of personal
data, as well as local acts establishing procedures aimed at preventing and identifying violations
of the legislation of the Russian Federation, eliminating the consequences of such violations. 4.7. The operator takes the necessary legal, organizational and technical measures or ensures their adoption to protect personal data from unauthorized or accidental access to it, destruction, modification, blocking, copying, provision, distribution of personal data, as well as from other unlawful actions in relation to personal data in in accordance with Article 19 of the Federal Law of July 27, 2006 No. 152-FZ "On Personal Data", including: 1) identification of threats to the security of personal data during their processing in personal data information systems; 2) application of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems necessary to fulfill the requirements for the protection of personal data, the implementation of which ensures the levels of personal data security established by the Government of the Russian Federation; 3) the use of information security means that have passed the compliance assessment procedure in accordance with the established procedure; 4) assessment of the effectiveness of measures taken to ensure the security of personal data before the commissioning of the personal data information system; 5) accounting of computer storage media of personal data; 6) detecting facts of unauthorized access to personal data and taking
measures; 7) restoration of personal data modified or destroyed due to unauthorized access to it; 8) establishing rules for 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 the measures taken to ensure the security of personal data and the level of security of personal data information systems. 4.8. The operator carries out internal control and (or) audit of compliance of the processing of personal data with the Federal Law of July 27, 2006 No. 152-FZ "On Personal Data" and the regulatory legal acts adopted in accordance with it, protection requirements

personal data, the operator's policy regarding the processing of personal data, local acts of the operator. 4.9. The operator assesses the harm that may be caused to
personal data subjects in the event of a violation of this Federal Law, the relationship between this harm and the measures taken by the operator aimed at ensuring the fulfillment of the obligations provided for by this Federal Law; 4.10. Familiarizes employees directly involved in the processing of personal data with the provisions of the legislation of the Russian Federation on personal data, including requirements for the protection of personal data, documents defining the operator's
policy regarding the processing of personal data, local acts on the processing of personal data, and (or) training of these employees; 4.11. Responsible persons of the relevant departments that store personal data on paper and machine media ensure their protection from unauthorized access and copying in accordance with the "Regulation on the specifics of processing personal data carried out without the use of automation tools", approved by Decree of the Government of the Russian Federation on September 15, 2008 No. 687. 4.12. Responsible persons of structural divisions processing personal data in personal data information systems and computer
storage media provide protection in accordance with the Decree of the Government of the Russian Federation of November 1, 2012 No. 1119 "On approval of requirements for the protection of personal data during their processing in personal data information systems "and other normative, normative-methodological, methodological documents. 4.13. Where possible, personal data should be anonymized. 4.14. Threat analysis. Ensuring the security of personal data, as well as the development and implementation of means of protecting personal data, is based on an analysis of threats to the security of personal

data.
the company, if necessary, develops and maintains a Private Threat Model for the security of personal data during its processing in personal data information systems (hereinafter referred to as the Private Threat Model). The private threat model reflects the current state of security of personal data information systems and current threats
to the security of personal data. The development of a Private Threat Model is carried out on the basis of an analysis of existing security threats and the possibility of their implementation in the personal data information systems being examined. 4.15. Procedure for destruction of personal data. The person responsible for the destruction of personal data is an authorized person appointed by order of the General Director. The authorized person is the chairman of the Company's commission for the destruction of personal data. The appointment of a commission for the destruction of personal
data is made by order of the director. Upon the occurrence of any of the events that entail, according to the legislation of the Russian Federation, the need to destroy personal data, the
Authorized Person is obliged to: - notify the members of the commission about the work to destroy personal data; - determine (assign) the time and place of work of the commission (time and place of destruction of personal data); - establish a list, type, name, registration numbers and other data of the
media on which the personal data subject to destruction is located (and/or physical media of personal data); - determine the technology (technique, method) of destruction of personal data (and/or material media of personal data);

- determine the technical (material, software and other) means by which personal data will be destroyed; - supervising the work of the commission
members, destroy personal data (and/or tangible media of personal data); - draw up the appropriate Act on the destruction of personal
data (and/or material media of personal data) and submit the Act on the destruction of personal data (and/or material media of personal data) for approval by the director; - if necessary, notify the subject of personal data and/or the authorized body about the destruction of
personal data.

V. RIGHTS AND OBLIGATIONS OF AN EMPLOYEE

5.1. Employees and their representatives must be familiarized, against receipt, with the Company's documents establishing the procedure for processing personal data of employees, as well as their rights and obligations in this area. 5.2. In order to protect personal data stored by the employer, the employee
has the right to: demand the exclusion or correction of incorrect or incomplete personal data; to free and free access to your
 personal data, including the right to receive

copies of any record containing personal data;
 personal data of an evaluative nature should be supplemented with a statement expressing his own point of view; identify your representatives to protect your
 personal data; to preserve and protect their personal and family secrets. 5.3. The employee is obliged:

 transfer to individual entrepreneur "Chachina Irina Gennadievna" and (or) its representative a complex of reliable, documented personal data, the composition of which is established by the Labor Code of the Russian Federation. promptly inform individual entrepreneur "Chachina Irina Gennadievna"
 about changes in your personal
data.
5.4. Employees notify the company of changes in last name, first name, patronymic, and date of birth, which is reflected in the work book based on the submitted documents. If necessary, information about education, profession, specialty,
assignment of a new category, etc. is changed. 5.5. In order to protect privacy, personal and family secrets, employees have the right to refuse to process personal data without their consent.

VI. RIGHTS AND OBLIGATIONS OF CLIENTS AND CONTRACTORS

6.1. In order to ensure the protection of personal data stored by the Operator, clients and counterparties have the right to: 6.1.1. Complete information about the
composition of personal data and its processing, in particular, the client or counterparty has the right to know who is using or has used information about his personal data and for what purposes. 6.1.2. Free free access to your personal data, including the right to receive copies of any record
containing personal data of a client or counterparty, except in cases provided for by the legislation of the Russian Federation. 6.1.3. Determining your representatives to protect your personal data. 6.1.4. Request for the exclusion or correction of incorrect or incomplete, outdated, unreliable, illegally obtained or not necessary personal data for the Operator. If the Operator
refuses to exclude or correct the personal data of a client or counterparty, he has the right to declare in writing to
the Operator his disagreement with the appropriate justification for such disagreement.

6.1.5. The requirement that the Operator notify all persons who were previously informed of incorrect or incomplete personal data of the client or counterparty of all exceptions, corrections or additions made to them. 6.1.6. Appeal to the court against any unlawful actions or inaction of the Operator during the processing and
protection of his personal data. 6.2. In order to ensure the reliability of personal data, the client and counterparty are obliged to: 6.2.1. When concluding an agreement, provide the Operator
with complete and reliable information about yourself; 6.2.2. In case of changes in the information constituting the personal data of the client or counterparty, immediately, but no later than five working days, provide this information to the Operator.

VII. RESPONSIBILITY FOR DISCLOSURE OF CONFIDENTIAL INFORMATION RELATED TO PERSONAL DATA OF EMPLOYEES

7.1. Legal entities and individuals, in accordance with their powers, possessing information about citizens, receiving and using it, are responsible in accordance with the legislation of the Russian Federation for violating the regime of protection, processing and procedure for using this information. 7.2. A manager who authorizes an employee's access to a confidential document is personally responsible for this permission. 7.3. Each employee of the organization
who receives a confidential document for work bears sole responsibility for the safety of the medium and the confidentiality of the information. 7.4. Persons guilty of violating the rules governing the receipt,
processing and protection of personal data bear disciplinary, administrative, civil or criminal liability in accordance with the legislation of the Russian Federation. 7.4.1. For failure or improper fulfillment by an employee, through his fault, of the duties assigned to him
to comply with the established procedure for working with confidential information, the company has the right to apply disciplinary sanctions provided for by the Labor Code of the Russian Federation. 7.4.2. Officials whose duties include the processing of personal data are obliged to provide everyone with the opportunity to familiarize themselves with documents and materials that
directly affect their rights and freedoms, unless otherwise provided by law. Unlawful refusal to provide documents collected in the prescribed manner, or untimely provision of such documents or other information in cases provided for by law, or provision of incomplete or knowingly false information - entails the imposition of an administrative fine on officials in the amount determined by the Code of Administrative Offenses. 7.4.3. In accordance with the Civil Code,
persons who obtained information constituting an official secret through illegal methods are obliged to compensate for the losses caused, and the same obligation is assigned to employees. 7.4.4. Criminal liability for violation of privacy (including illegal collection or dissemination of information about the private life of a person, constituting his personal or family secret, without his consent), unlawful access to legally protected computer information, unlawful refusal to provide documents collected in the prescribed manner and information (if these acts caused harm to the rights and legitimate interests of citizens), committed by a person using his official position, is punishable by a fine, or deprivation of the right to hold certain positions or engage in certain activities, or arrest. 7.5. The illegality of the activities of government bodies and organizations in the collection and use of personal data can be established in court.

VIII. RESPONSIBILITIES OF EMPLOYEES TO PROTECT CONFIDENTIAL INFORMATION

8.1. In order to protect the confidentiality of information, all employees are obliged to: 8.1.1. Do not disclose information that constitutes a trade secret of IP “Chachina Irina Gennadievna”, except in cases where there is written consent. 8.1.2. Do not use information that constitutes a trade secret of IP “Chachina Irina Gennadievna” to engage in other activities, in the process of working for another organization, enterprise, institution, on the instructions of an individual or in the course of business activities, as well as for personal purposes. 8.1.3. Comply with the trade secret regime established by the company. 8.1.4. Immediately notify the immediate supervisor and director of the Company about the need to answer or answer questions from officials of the competent authorities (tax inspectorate, preliminary investigation bodies, etc.) who are on duty regarding the Company’s trade secrets. 8.1.5. Immediately inform your immediate supervisor and Irina Gennadievna Chachina about the loss or shortage of media containing information constituting a trade secret, certificates, passes, keys to premises, storage facilities, safes, personal seals and other facts that may lead to the disclosure of a trade secret of IP "Irina Gennadievna Chachina" , as well as the reasons and conditions for a possible leak of information constituting a trade secret. 8.1.6. If unauthorized persons attempt to obtain from an employee information containing a company trade secret, immediately notify the immediate supervisor and Chachina Irina Gennadievna. 8.1.7. Not to create conditions for the leakage of information constituting a trade secret, and to make every effort to suppress such a leak if he becomes aware that a leak is taking place or that conditions are developing for the possibility of such a leak. 8.1.8. Do not disclose or use trade secrets for yourself or other persons for five years after termination of your employment contract with the company (regardless of the reasons for dismissal). 8.1.9. Transfer to individual entrepreneur “Chachina Irina Gennadievna” upon termination of an employment contract or civil contract the material media in the employee’s use containing information constituting a trade secret.

IX. FINAL PROVISIONS

9.1 These Regulations come into force from the moment of its approval by Individual Entrepreneur “Chachina Irina Gennadievna."

9.2 These Regulations are brought to the attention of all employees of the company personally against signature.