On approval of the Rules for provision of microcredits electronically

Unofficial translation

Resolution of the Board of the National Bank of the Republic of Kazakhstan dated November 28, 2019 № 217. Registered with the Ministry of Justice of the Republic of Kazakhstan on December 6, 2019 № 19714.

Unofficial translation

In accordance with the Law of the Republic of Kazakhstan "On Microfinance Activities", the Board of the National Bank of the Republic of Kazakhstan **HEREBY RESOLVES**:

Footnote. Preamble - as amended by the Resolution of the Board of the Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market № 81 dated 3010.2023 (shall come into effect ten calendar days after the day of its first official publication).

1. To approve the attached Rules for the provision of microcredits electronically.

2. The Department of methodology and regulation of financial organizations, in accordance with the procedure, established by the legislation of the Republic of Kazakhstan shall ensure:

1) jointly with the Legal Department, the state registration of this resolution with the Ministry of Justice of the Republic of Kazakhstan;

2) placement of this resolution on the official Internet resource of the National Bank of the Republic of Kazakhstan after its official publication;

3) within ten working days after the state registration of this resolution, submission to the Legal Department of information about implementation of measures, stipulated by subclause 2) of this clause and clause 3 of this resolution.

3. The Department of External Communications – the Press Service of the National Bank shall ensure, within ten calendar days after the state registration of this resolution, sending of its copy for official publication to printed periodicals.

4. Control over execution of this resolution shall be entrusted to the deputy Chairman of the National Bank of the Republic of Kazakhstan Smolyakov O.A.

5. This resolution shall come into force from January 1, 2020 and shall be subject to official publication.

Chairman
of the National Bank *Ye. Dossayev*

Approved
by the Resolution of
the National Bank

of the Republic of Kazakhstan
dated November 28, 2019
№ 217

The Rules for the provision of microcredits electronically

Footnote. The rules are as amended by Resolution № 81 of the Board of the Agency for Regulation and Development of the Financial Market of the Republic of Kazakhstan dated 30.10.2023 (effective ten calendar days after the date of its first official publication).

Chapter 1. General Provisions

1. These Rules for the provision of microcredits electronically (hereinafter referred to as the Rules) have been developed in accordance with paragraph 3-1 of Article 3 of the Law of the Republic of Kazakhstan "On Microfinance Activities" (hereinafter referred to as the Law) and shall determine the procedure for providing microcredits electronically.

2. The Rules shall use the concepts provided for by the Law, as well as the following concepts:

1) automated information system - an information system that automates the provision of microcredits electronically in an organization engaged in microfinance activities;

2) authentication - a procedure for verifying the authenticity of the client, electronic messages and other documents, including electronic copies of documents necessary to provide microcredit, as well as identifying the client and the content of his/her expression of will;

3) debt - the amount of debt on microcredit, including the amount of the principal balance, accrued but unpaid remuneration, penalties (fines, penalties) provided for in the microcredit agreement concluded with the borrower;

4) biometric identification – a set of measures that identify a person based on physiological and biological immutable characteristics;

5) one-time password – a password valid only for one authentication session of subjects receiving services in electronic form;

6) two-factor authentication – authentication carried out using two of three different factors: knowledge, ownership, inalienability;

7) personal account – a multifunctional secure service of an automated information system that ensures interaction between an organization carrying out microfinance activities and a client;

8) client - an individual or legal entity who has agreed with an organization engaged in microfinance activities to provide microcredit or has submitted (intends to submit) an application for microcredit;

9) client identification – the procedure for the client to provide his/her identification data for further authentication;

10) mobile application - a software product used on a subscriber's cellular device and providing access to a personal account via cellular services or the Internet;

11) identifier - a unique digital, alphabetic or containing other symbols code assigned to the client to enter his/her personal account;

12) identification data exchange center (IDEC) - an operational center of the interbank money transfer system, ensuring interaction with financial organizations for the exchange of customer data from available sources for carrying out customer identification procedures;

13) smart card – a plastic card with a built-in microcircuit;

14) terminal – an electronic-mechanical device designed to carry out operations related to the provision of microcredits;

15) token – a device designed to ensure the information security of the user, as well as to identify its owner, and secure remote access to information resources;

16) authorized body - a state body that carries out state regulation, control and supervision of the financial market and financial organizations;

17) "electronic government" web portal - an information system that is a single window of access to all consolidated government information, including the regulatory legal framework, and to government services, services for issuing technical specifications for connecting to the networks of natural monopoly entities and services of quasi-state entities sector, provided in electronic form.

Chapter 2. Providing microcredits electronically

3. Operations related to the provision of microcredits electronically shall be carried out using an automated information system that meets the requirements of Chapter 3 of these Rules in the client's personal account on the Internet resource, in a mobile application and (or) terminals of an organization carrying out microfinance activities.

4. 10 (ten) working days before the opening of an Internet resource, mobile application and (or) terminal through which microcredits shall be provided electronically, the organization carrying out microfinance activities shall notify the authorized body about this.

The notification sent to the authorized body shall contain:

1) name of the Internet resource, mobile application and (or) location of the terminal of the organization carrying out microfinance activities;

2) a list of services (operations) that can be provided through an Internet resource, mobile application and (or) terminal of an organization engaged in microfinance activities;

3) information about the availability of approved procedures for the security and protection of information from unauthorized access by an organization engaged in microfinance activities when providing services through an Internet resource, mobile application and (or) terminal, with supporting documents attached.

5. If the information contained in the notification specified in paragraph 4 of the Rules changes, the organization carrying out microfinance activities notifies the authorized body 10 (ten) working days before such changes are made.

6. To register in the personal account, a client - an individual shall enter (attach) the following data:

last name, first name, patronymic (if any) indicated in the identity document, except for the birth certificate;

individual identification number;

number and validity period of the identity document, except for the birth certificate;

subscriber number of the cellular communication device;

photo of a client in full face on a bright background, with a neutral expression on his face and a closed mouth.

To register in the personal account, a client-legal entity shall enter (attach) the following data (scanned documents):

order appointing the head of the executive body of a legal entity or a power of attorney confirming the powers of the person authorized to sign an agreement on the provision of microcredit;

last name, first name, patronymic (if any) indicated in the identity document, except for the birth certificate, of the person authorized to sign the microcredit agreement;

business identification number of the client - legal entity;

the microcredit agreement;

number and validity period of the identity document, except for the birth certificate, of the person authorized to sign the microcredit agreement;

subscriber number of the cellular communication device of the client - legal entity;

photo of a client in full face on a bright background, with a neutral expression on his face and a closed mouth, authorized to sign an agreement on the provision of microcredit.

An organization carrying out microfinance activities, to confirm client registration, shall verify the data provided by:

client - an individual: last name, first name, patronymic (if any), individual identification number and photograph of the client;

client - a legal entity: last name, first name, patronymic (if any) and photograph of the person indicated in the identification document, except for the birth certificate, of the person authorized to sign the microcredit agreement.

Client registration in the personal account shall be carried out using at least two authentication methods specified in paragraph 35 of the Rules, one of which is biometric identification.

After registering a client in his/her personal account, the client's subsequent access to his/her personal account shall be carried out by generating and (or) entering passwords or using at least one of the authentication features (tokens, smart cards, one-time passwords).

Changes to the subscriber number of the client's cellular communication device and bank account details (except for the provision of microcredits through terminals) shall be made in the client's personal account using one of the authentication methods specified in paragraph 35 of the Rules.

In the personal account, data on the client’s individual identification number or business identification number cannot be changed.

7. The personal account must provide the client with the opportunity to perform the following, but not limited to, actions:

1) submission of an application by a client for microcredit;

2) viewing information about the organization carrying out microfinance activities (legal and (or) actual address, contact numbers, fax, email address and other information), information about the first manager (last name, first name, patronymic (if any) of the organization carrying out microfinance activity;

3) review of the client’s agreement (agreements) on the provision of microcredit (before and after agreeing);

4) viewing information on the progress and results of consideration of the client’s application for microcredit;

5) viewing information about the amount of the client’s current debt under microcredit (microcredits), upcoming and actual payments by the client, including the amount of the principal debt, remuneration, penalties (fines, forfeit);

6) viewing information about ways to repay microcredit by a client;

7) exchange of letters (messages) between the client and the organization carrying out microfinance activities.

8. Before providing microcredit electronically, an organization carrying out microfinance activities shall:

1) carry out due diligence of the client in accordance with the legislation of the Republic of Kazakhstan in the field of combating the legalization (laundering) of proceeds from crime and the financing of terrorism and internal documents;

2) familiarize the client with the Rules for the provision of microcredits;

3) provide the client with complete and reliable information about payments and transfers related to the receipt, servicing and repayment (return) of microcredit;

4) provide the client with draft repayment schedules calculated by various methods (differentiated payments method, annuity payments or a method calculated in accordance with the Rules for provision of microcredits) for review and selection of microcredit repayment method;

5) inform the client about his/her rights and obligations related to receiving microcredit;

6) request from the client a method for providing microcredit (by issuing cash to the client through a terminal or cash desk, or transferring microcredit to the bank account (payment card) of the client or the bank account of a legal entity with which the organization carrying

out microfinance activities has concluded an agreement providing for payment for goods purchased or work performed, services performed by the borrower);

7) request bank account details (IBAN) and (or) details of the client's payment card, in case of providing microcredit to the client's bank account (payment card).

9. The conclusion of an agreement on the provision of microcredit, the introduction of amendments and additions to the agreement on the provision of microcredit electronically between an organization engaged in microfinance activities and the client shall be carried out through client authentication using at least two methods specified in paragraph 35 of the Rules.

Providing microcredit electronically shall be carried out by transferring money from the bank account of an organization carrying out microfinance activities to the bank account (payment card) of the client, as well as by issuing cash to the client through a terminal or cash desk and (or) transferring microcredit at the request of the borrower to the bank account of a legal entity. a person with whom an organization engaged in microfinance activities has entered into an agreement providing for payment for goods purchased or work performed or services performed by the borrower.

Transfer of microcredit at the request of the borrower to the bank account of a legal entity with which the organization carrying out microfinance activities has concluded an agreement providing for payment for the purchased goods or work performed, services performed by the borrower, shall be carried out through client authentication using at least two authentication methods indicated in paragraph 35 of the Rules.

Providing microcredit to a borrower through a cash desk shall be carried out by visually identifying the client receiving cash with an identification document, except for a birth certificate, or data confirming (identifying) the client's identity obtained through the digital document service.

10. An organization carrying out microfinance activities shall refuse to provide microcredit to a client on the grounds provided for by the legislation of the Republic of Kazakhstan in the field of combating the legalization (laundering) of proceeds from crime and the financing of terrorism.

11. The provision of microcredits electronically shall be carried out in accordance with the internal documents of the organization carrying out microfinance activities, which provide for the identification of distortions and (or) changes in the content of electronic documents on the basis of which the client was granted microcredit electronically, as well as protection from unauthorized access to information constituting the secrecy of providing microcredit, and the integrity of this information, including the protection of identification and authentication data provided by the client from repeated unauthorized use when receiving microcredit.

12. At the request of the client, the organization carrying out microfinance activities shall provide him/her with confirmation of the sending and (or) receipt of electronic documents

confirming the provision (receipt) of microcredit electronically, in the manner and within the time frame provided for in the microcredit agreement.

13. In case of detection of unauthorized access to information that constitutes the secret of providing microcredit, its unauthorized modification, unauthorized actions by third parties or other illegal (fraudulent) actions with microcredits, the organization carrying out microfinance activities shall take measures within two working days to eliminate the causes and consequences of such actions, and shall also inform the client and the authorized body about this within one working day.

If a person conducting a pre-trial investigation in accordance with Article 200 of the Criminal Procedure Code of the Republic of Kazakhstan (hereinafter referred to as the Code of Criminal Procedure of the Republic of Kazakhstan) submits to an organization engaged in microfinance activities a proposal to take measures to eliminate the circumstances that contributed to the commission of a criminal offence against victims, or resolution on recognizing the borrower of an organization engaged in microfinance activities as a victim in accordance with Article 71 of the Code of Criminal Procedure of the Republic of Kazakhstan, an organization engaged in microfinance activities, no later than 3 (three) working days from the date of receipt of the submission or resolution shall:

suspend the accrual of interest on such microcredit;

suspend debt collection and claims work on microcredit;

suspend sending information to credit bureaus about the client's debt on microcredit;

send a written notification to the client about the suspension of the accrual of remuneration on the microcredit, debt collection and carrying out claim work on the client.

In the event of cancellation by an authorized person or body of submission or resolution based on which the accrual of remuneration on microcredit, debt collection and the conduct of claims work shall be suspended, the organization engaged in microfinance activities shall have the right to additionally accrue remuneration for the use of microcredit for the period of suspension of the accrual of remuneration, and resume debt collection and claim work for the client.

Based on a court verdict that has entered into legal force, which established the fact that the client did not receive microcredit, an organization engaged in microfinance activities, within 15 (fifteen) working days shall:

make a decision to write off the client's debt under this microcredit;

make adjustments to the client’s credit history in credit bureaus by sending information about the absence of debt on this microcredit and the number of overdue days on it;

return to the client amounts of debt under this microcredit, previously collected by the organization carrying out microfinance activities, or repaid by the client independently.

Write-off of a client's debt on microcredit, in accordance with this paragraph of the Rules, shall not deprive an organization engaged in microfinance activities of the right to demand from the client compensation of debt on microcredit issued to him, issued fraudulently if the client himself is at fault, established by the court.

Chapter 3. Requirements for an automated information system

14. The automated information system shall include:

1) web application server software (hereinafter referred to as the Web application);

2) software for mobile devices (hereinafter referred to as the Mobile application);

3) software for software interface servers (hereinafter referred to as Server software).

15. Development and (or) modification of an automated information system shall be carried out by an organization carrying out microfinance activities in accordance with an internal document regulating the procedure for development and (or) modification, stages of development and their participants.

16. If the development and (or) modification of an automated information system is transferred to a third-party organization and (or) a third party, the organization carrying out microfinance activities shall ensure that the third-party organization and (or) third party fulfils the requirements of this chapter and internal documents, and shall be responsible for security status of the automated information system.

17. Storage of the source codes of the automated information system developed in an organization carrying out microfinance activities shall be carried out in specialized code repository management systems located within the security perimeter of the organization carrying out microfinance activities, with backup provided.

18. Regardless of the approach adopted in an organization carrying out microfinance activities to the development and (or) modification of an automated information system, a mandatory stage is security testing, during which at least the following activities shall be carried out:

1) static analysis of source code;

2) analysis of components and (or) third-party libraries.

19. Static analysis of the source code of an automated information system shall be carried out using a static source code analysis scanner, which supports the analysis of all programming languages used in the software being tested, the functions of which include identifying the following vulnerabilities, but not limited to:

1) the presence of mechanisms that allow the injection of malicious code;

2) use of vulnerable operators and functions of programming languages;

3) use of weak and vulnerable cryptographic algorithms;

4) use of code that, under certain conditions, causes a denial of service or a significant slowdown in the operation of the application;

5) the presence of mechanisms to bypass application security systems;

6) use of secrets in clear text in the code;

7) violation of application security patterns and practices.

20. Analysis of components and (or) third-party libraries of an automated information system shall be carried out to identify known vulnerabilities inherent in the version of the component and (or) third-party library used, as well as to track dependencies between components and (or) third-party libraries and their versions.

21. An organization carrying out microfinance activities shall ensure the implementation of corrective measures to eliminate identified vulnerabilities in the manner specified by the internal document, while critical vulnerabilities are eliminated before the automated information system and (or) its new versions are put into operation.

22. An organization carrying out microfinance activities shall provide storage and online access to all versions of the source codes of the automated information system and security testing results that have been put into operation over the past 3 (three) years.

23. Data exchange between the client and server sides of the automated information system shall be encrypted using a version of the Transport encryption protocolLayerSecurity (Transport Layer Security) not lower than 1.2.

24. The web application shall provide:

1) unambiguous identification of the ownership of the web application of an organization engaged in microfinance activities (domain name, logos, corporate colours);

2) prohibition on storing authorization data in the browser's memory;

3) masking of entered secrets;

cyber hygiene measures that are recommended to be followed when using the web application;

5) handling errors and exceptions securely, preventing sensitive data from being displayed in the client interface, and providing minimally sufficient information about the error.

25. The mobile application shall provide:

1) unambiguous identification of the ownership of a mobile application of an organization engaged in microfinance activities (data in the official application store, logos, corporate colours);

2) blocking the functionality for providing microcredits electronically to an organization engaged in microfinance activities, in case of detection of signs of integrity violation and (or) bypassing the security mechanisms of the operating system, detection of remote control processes;

3) notifying the client about the availability of updates to the mobile application;

4) the ability to force installation of mobile application updates or block the functionality of a mobile application before installing them in cases where it is necessary to eliminate critical vulnerabilities;

5) storing confidential data in a secure container of a mobile application or storage of system credentials;

6) exclusion of caching of confidential data;

7) exclusion of confidential data from backup copies of the mobile application;

8) informing the client about effective methods of ensuring cyber hygiene, which are recommended to be followed when using the mobile application;

9) informing the client about events of authorization under his account, changes and (or) recovery of the password, and changes in the mobile phone number registered by the organization carrying out microfinance activities;

10) during transactions with funds - transfer to the server software of an organization carrying out microfinance activities, geolocation data of a mobile device if there is permission from the client or transfer of information about the absence of such permission.

26. An organization carrying out microfinance activities shall provide on its side:

1) handling errors and exceptions securely, without disclosing confidential data in the response, providing minimally sufficient information to diagnose the problem;

2) identification and authentication of mobile applications and associated devices;

3) checking data for validity to prevent requests forgery and injection attacks.

27. Access to information in the automated information system shall be provided to employees of an organization carrying out microfinance activities to the extent necessary to perform their functional duties.

28. Access to the automated information system shall be carried out by identifying and authenticating employees of an organization carrying out microfinance activities.

29. The automated information system shall use functions for managing accounts and passwords, as well as blocking user accounts, determined by the internal document of the organization carrying out microfinance activities.

30. The automated information system shall be provided with technical support, which includes services for providing updates to the automated information system, including security updates.

31. The automated information system shall provide backup storage of data, files and settings, which ensures the restoration of its working copy.

32. In an organization carrying out microfinance activities, the maintenance and immutability of the audit trail of the automated information system shall be ensured, both at the organizational and technical levels.

33. To protect an automated information system, licensed anti-virus software or systems shall be used to ensure the integrity or control of the immutability of the software environment on workstations, laptops and mobile devices.

34. An organization engaged in microfinance activities ensures secure storage of electronic messages and other documents provided to and received from the client, maintaining their integrity and confidentiality for at least 5 (five) years after the termination of the obligations of the parties under the microcredit agreement.

Electronic messages and other documents shall be stored in the format in which they were generated, sent to the client or received from him/her.

35. To identify and authenticate a client in the client’s personal account, the following methods shall be used:

1) electronic digital signature of the client, presented by the national certification center of the Republic of Kazakhstan;

2) biometric identification of the client through the use of data center services;

3) two-factor client authentication.

Two-factor client authentication shall be achieved by applying at least two of the following factors:

confirmation of the knowledge factor: the client entering a password or code word independently specified during registration;

confirmation of the ownership factor: the client entering a one-time password automatically generated by a token registered with the client, or connecting a smart card registered with the client to the client reader, or entering a one-time password automatically generated and transmitted by the client to the subscriber number of the client’s cellular device specified by the client, with verification of the client's ownership of this subscriber number by checking the client's individual identification number with the individual identification number of the owner of the subscriber number in the database of the mobile operator or obtaining information about the client's ownership of this subscriber number by checking the client's individual identification number in the database of clients' mobile phone numbers via the web - “electronic government” portal;

confirmation of the inalienability factor: verification of the image of the client’s face in real-time with his/her image on an identity document, except for a birth certificate, which protects the use of a static image or video recording of the client’s face instead of a real-time image of the client’s face.