

According to the decision of the Executive Board of "AMIO BANK" CJSC dated
20.08.2025



**FACEPASS-AMIO Facial Payment Service, Card Linking, and Personal Data
Processing Terms and Conditions by "AMIO BANK" CJSC**

"AMIO BANK" CJSC

Address: Nalbandyan 48, Yerevan, RA

Phone: (+374 10) 592020, (+374 60) 37-25-00

info@amiobank.am

**Terms and Conditions for Registration of Facial Biometric Data and Card Linking on the
FACEPASS-AMIO Remote Platform of "AMIO BANK" CJSC**

Nature of the Service:

1. The FacePass-AMIO remote platform of AMIO Bank (hereinafter referred to as the Bank) (hereinafter referred to as the System) allows users to register in advance, store their facial biometric data, and link a bank card for the purpose of making payments through facial recognition in the future (hereinafter referred to as the Service).
2. You can register a personal account in the system by entering your email address and a password of your choice.
3. Based on the information you provide, the Bank will collect and register your data in its database for the purpose of making payments through facial recognition, in which case the payment amount will be deducted from the previously linked bank card.

Essential terms of the service:

4. It is possible to link Mastercard cards in AMD, USD, EUR, or RUB currencies issued by AMIO Bank or other banks (whether in Armenia or abroad) to the system (hereinafter referred to as the Issuing Bank), excluding the Bank's business and children's cards.
5. When linking the card, an amount of 100 AMD will be charged from the card for verification purposes, which will be refunded within a few minutes.
6. To ensure the security of the card linking process, the 3D Secure technology (Mastercard Secure Code) is used, in accordance with the rules set by the Bank, by entering a one-time password provided to the cardholder by the Issuing Bank.
7. After the card is linked, its details will be stored in the Bank's database to ensure its future use.
8. Only one card is allowed to be linked to the system. To link another card, the previously linked card must first be removed.
9. The encrypted details of the linked card are displayed on the Main page of the Bank's System.
10. The attached card can be used to make cashless payments at trade and service points operating in the territory of Armenia that have FacePass-AMIO payment capabilities.
11. Transactions made through the FacePass-AMIO payment platform are equivalent to transactions made with the card.

12. The fees, service conditions, and usage rules applicable to the card are regulated within the scope of the agreement between you and the card-issuing bank.
13. The Bank does not charge any additional fees for registering the card in the System, performing other operations, or making payments through the FacePass-AMIO payment platform.
14. If the currency of the linked card differs from the currency of the payment, the conversion transaction is carried out by the card's Issuing Bank in accordance with the terms and conditions set by that bank.
15. The Bank has the right to refuse the registration or use of the card in cases such as the card being blocked, suspected fraud, or other similar situations.
16. To contact you, the Bank may use any address/contact method/phone number that you specified during registration in the System.
17. In case of registration in the System, login to the System or changing registered data, the Bank has the right to send you passwords/codes via e-mail or SMS message to verify your identity.
18. The Bank has the right to require the creation of a graphical password (PassKey) in the System, at your discretion, for the purpose of confirming a transaction at the time of payment through the FacePass-AMIO payment platform.
19. The Bank reserves the right to reject the payment transaction.
 - 1) In case of providing inaccurate or unreliable information.
 - 2) In case of failure to pass facial biometric verification — when the face captured at the time of payment does not match the face previously registered in the System.
 - 3) In case of non-compliance with other terms and conditions of the Bank/service.
20. In case of transaction cancellation, according to the software solution, the sales point employee performs the cancellation in the cash register system. After that, the process is carried out in accordance with the standard procedure applicable to the cancellation of card transactions.

Your Responsibility:

20. You are responsible for registering your card in the System, for the payments and transactions made with the registered card, as well as for maintaining the confidentiality of any information that enables the use of the card or the System, such as access to the System, passwords sent via SMS, and similar data.
21. You are obliged to immediately inform the Bank about the need to block the ability to perform transactions using the card registered in the System, if:
 - you have lost your card,
 - you have lost the device on which you receive passwords,
 - access to the System (usage credentials) has become known or may become accessible to a third party.

22. You are also required to immediately notify the card-issuing bank about the need to block the card.

NOTICE AND CONSENT FOR PROCESSING PERSONAL AND BIOMETRIC DATA

This Notice and Consent to process personal and biometric data (hereinafter referred to as the Notice and Consent) is provided in accordance with the RA Law on “Personal Data Protection” (hereinafter referred to as the Law). Personal and biometric data processor or Bank: "AMIO BANK" CJSC, address: 48 Nalbandyan Street, Yerevan, Republic of Armenia.

By reviewing this Notice and Consent on the Bank's remote platform and approving it by ticking the "V" symbol, you confirm that you are aware of this Notice and Consent and consent to the Bank processing your personal and biometric data, namely: name, surname, telephone number, biometric data (face, fingerprint, etc.), which allow for direct or indirect identification of the client's identity in accordance with the Law.

Your personal and/or biometric data will be processed for the purpose of using the Service to make non-cash payments, to use the services provided by the Bank in the future, and to receive information about promotions/offers/other services conducted by the Bank.

Consent to the processing of personal and biometric data is given in accordance with the Law to perform such actions with your personal and/or biometric data (collection, recording, input, systematization, storage, use, etc.) that are necessary to achieve the purposes specified in this Notice and Consent and to fulfill the obligations imposed on the Bank by law.

On approving this Notice and Consent by ticking the "V" symbol on the Bank's remote platform, you allow and authorize the Bank to transfer your personal and biometric data for the purpose of online identification and transaction processing to organizations related to the "Sumsb" group of companies, which are obliged to implement appropriate technical and organizational measures to ensure the security of personal and biometric data in order to achieve the goals specified in this Notice and Consent.

Consent to the processing of personal and biometric data is deemed to be given by you upon reviewing the Notice and Consent and approving it by ticking the "V" symbol, and the Bank receives the right to process your personal and biometric data for the purposes specified in this Notice and Consent, as well as for the purpose of providing it to organizations cooperating with the Bank/providing services to the Bank/performing work for the Bank in accordance with the RA Law "On Banking Secrecy", provided that this is necessary for providing the given services or performing the work and/or in all cases where the requirement for processing such data is directly stipulated by law.

This Notice and Consent shall be deemed valid even in the event of renaming, reorganization, or replacement of the above-mentioned entities that serve as sources of the aforementioned data, provided that the scope of information to be received or disclosed on the basis of this Notice and Consent remains unchanged.

In the event of your written withdrawal of consent to the processing of your personal and biometric data, or a request for the correction or destruction of personal and/or biometric data (if the personal and/or biometric data are incomplete or inaccurate or outdated or obtained unlawfully

or are not necessary to achieve the purposes of processing). The Bank undertakes to terminate the processing of your personal and/or biometric data or to correct or destroy your personal and/or biometric data within ten business days, if there are no unfulfilled obligations and/or no existing contractual relations between you and the Bank, otherwise the contractual relations between you and the Bank are subject to termination with all the negative consequences arising therefrom. In case of withdrawal of consent to the processing of your personal and biometric data or request the destruction of your personal and/or biometric data, your personal and/or biometric data will cease to be processed by the Bank, but they will be stored in the information archive and may be used only in cases provided for by law. Withdrawal of consent is not retroactive.

Consent to the processing of personal and biometric data is given for the purpose of making payments using biometric data and remains valid for the entire period of provision of the Service, and in cases specified by law, for the period specified for those cases.

This Consent shall also be deemed granted in the event of renaming, reorganization, or replacement of the above-mentioned entities serving as sources of the aforementioned data, provided that the scope of information to be received or disclosed on the basis of this Consent remains unchanged.