Privacy policy of digitization of cards issued by "ACBA BANK" Open Joint-Stock Company (OJSC) in third-party wallets and Payments made by digitized cards

1. The main principles

1.1 ACBA BANK Open Joint-Stock Company (hereinafter referred to as the Bank) undertakes to maintain the security of its Customers' personal data, which are available in the Bank's databases. This Privacy Policy document provides Customer information that may be transferred from the Bank's database to third-party wallets (hereinafter referred to as the Payment Application) or used by the Bank.

1.2 This document also presents the points to be performed by the Customer, which are the most important means of data protection.

2. Obtaining customer data, purposes of the use

2.1 The use of the Customer's personal data is carried out exclusively within the limits of the Banking Law.

2.2 The Bank has the right to transfer the Customer data to the Payment Application during the card digitization process, and after that:

- Customer name / surname
- Card numbers,
- Card validation period, type of payment system, card design.

The above data will be used by the Payment Application exclusively for transactions with digital card and to make inquiries to the Bank.

2.3 The Bank has the right to send information about digitized card transactions, change of digitized card status, as well as messages about marketing offers and campaigns to Customer's phone number registered in the Bank.

2.4 The Bank has the right to receive and save the following data about mobile phone in the Bank database during the digitization of the card:

- Mobile phone model,
- IP address,
- Operating system version
- Mobile phone unique identification data

The above data will be used exclusively for technical improvements, problem solving or targeted marketing campaigns.
2.5 The Bank has the right to keep digitized card transactions in the Bank's database, in particular:
- Transaction number,
- Place of the transaction,
- Amount of the transaction,
- Transaction status,
- Terminal ID

The above data will be used exclusively for technical improvements, problem solving or targeted marketing campaigns.

### 3. Security

3.1 In order to minimize the risk of fraud and data theft, the Customer is strongly advised to comply with the requirements set out below.

3.1.1 Create a complex password / PIN code on your mobile phone,
3.1.2 Do not leave the unlocked cell phone with other people,
3.1.3 Provide safer unlocking methods on your mobile phone: FaceID, TouchID,
3.1.4 Make sure that other people do not have biometric identification data in your phone settings;
3.1.5 Do not provide the Payment application password / PIN code with other persons,
3.1.6 Do not share the username, password and PIN code of the acba digital application with others.
3.1.7 In case of suspicion that another person possesses information about items 3.1.4, 3.1.5, 3.1.6 points, make appropriate changes.
3.1.8 Remove all identification data from the mobile phone settings: FaceID, TouchID, password & PIN code, if the mobile phone is no longer used by the Customer.

3.2 In case of loss of mobile phone, suspicious transactions, it is necessary to immediately inform the Bank, after which the Bank will block the digitized card.

### 4. Changes to the terms of the Privacy Policy

4.1 The Bank has the right to make changes to the Privacy Policy in this document without additional approval by the Customer.

4.2 The Bank undertakes to publish the changed data on its official website: acba.am.
4.3 The Bank may, at its discretion, send the new edition of the Privacy Policy clauses to the Customer's e-mail address registered in the Bank.