TERMS AND CONDITIONS FOR THE USE OF THE OPEN BANKING SERVICE

Definitions:

- **Third Party Provider (TPPs)** – are entities that offer payment services but do not hold the customer's funds.
- **Payment Initiation Service Provider (PISP)** – is a third-party provider that facilitates direct online payments from a customer's bank account to a merchant or a service provider.
- **Account Information Service Providers (AISP)** – is a third-party provider authorized to access and retrieve financial data from a customer's bank account but not process transactions.
- **Payment Service User (PSU)** – refers to any individual or entity that uses a payment service.
- **Account Servicing Payment Service Provider** (referred to as "the Bank" or "BKT") that offers a dedicated API interface as stipulated in article 35 of Regulation no. 29/2022 "On strong customer authentication and common, open and secure standards of communication".
- **Application Programming Interface (API)** – is a standardized interface that allows TPP, PISP, AISP to securely access and interact with a customer's bank account information.
- **Payment Beneficiary** - refers to the individual or entity that receives the funds from a payment transaction.
- **SCA (Strong Customer Authentication)** – refers to the method of customer authentication applied an all open banking channels in compliance with provision of Regulation no. 29/2022 "On strong customer authentication and common, open and secure standards of communication".
- **SLA (Service Level Agreement**) – document defining the level of service and service recovery standards.
- **Applicant –** All institutions (TPP, PISP, AISP) that require the integration with API interface provided by BKT in compliance with Open Banking regulatory framework.
- **The Parties** – Referring jointly to the bank and the applicant.

Introduction

This document sets out the terms and conditions governing access to and use of the Open Banking Service offered by Banka Kombëtare Tregtare sh.a. (hereinafter "BKT") by authorized third-party providers (Third Party Providers – TPPs), in accordance with the provisions of Law No. 55/2020 "On Payment Services" and the regulatory framework of the Bank of Albania.

The use of this service requires the explicit and informed consent of the customer for the access to their financial data or for the initiation of payments through licensed third-party applications. The consent granted by the customer may be revoked at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

TPPs are required to possess qualified certificates (QWAC and/or QSEAL) in accordance with eIDAS standards and must have completed the integration and technical verification process

within BKT's sandbox environment prior to accessing the production environment.The applicant declares that they have been informed and accept that this service channel is dedicated to payments within the territory of Albania for all consumers (excluding legal entities) and that the activation of this service will be carried out only after the approval of the applicable terms and conditions set out in this document.

Access to BKT's Developer Portal

The BKT Developer Portal is offered at the sole discretion of Banka Kombëtare Tregtare, and any individual or entity wishing to gain access must register through the portal's official website. BKT reserves the right to review and approve or reject any registration application at its sole discretion and will inform accordingly on any refusal in compliance with legal framework.

The applicant declares that has obtained the relevant license from Bank of Albania or has successfully passed the process of reassessment stipulated in article 99 of the Law no. 55/2020 "On Payment Services" and will provide the relevant documentary evidence to BKT.

The applicant declares that they will collaborate with the bank in providing the necessary information or documentation (when required) as part of risk assessment processes during the application and integration phase.

All information provided during the registration process must be accurate, complete, and up to date. The applicant is responsible for maintaining and updating this information throughout the duration of their registration.

Upon successful registration, users may be provided with login credentials, passwords, or other identifying information ("Credentials"), which remain the property of BKT and are licensed to the user on a non-exclusive, non-transferable basis solely for the purpose of using the Developer Portal.

The user is obligated to maintain the confidentiality of these credentials and is not permitted to transfer, sell, sublicense, or otherwise disclose them to any third party. If the user suspects or becomes aware that the confidentiality of the credentials has been compromised, they must notify BKT without undue delay.

Any attempt to bypass or modify the credentials, authentication systems, or security mechanisms used by BKT in connection with the Developer Portal is strictly prohibited.

Rules for the Use of BKT's Developer Portal

The user is responsible for all activities carried out through the use of their Credentials, whether performed by the user themselves or by a third party. The user commits to comply with all legal requirements and to refrain from creating, distributing, or uploading content that is prohibited by law or may be considered inappropriate, offensive, or in conflict with institutional ethics. All actions taken within or in connection with BKT's Developer Portal must comply with BKT's Code of Conduct and Ethics as well as other relevant internal regulations.

The user is strictly prohibited from engaging in the following activities:

a) Attempting to analyze BKT's developer platform code through methods such as decompilation, reverse engineering, or any technique intended to discover or alter the technical operation of APIs, test data, or any other material provided by BKT under this portal;
b) Attempting unauthorized access to BKT systems or services, or using them in an unauthorized manner;
c) Damaging, disrupting, or negatively impacting the operation of BKT's systems or services;
d) Performing actions that prevent other users from accessing BKT's content;
e) Using bots or any automated application to scrape, copy, or index BKT's content;
f) Collecting data or information about other users of the Developer Portal;
g) Introducing viruses, malicious code, or other harmful elements into BKT systems.

Any violation of these rules may result in the immediate suspension of access, deletion of the user account from the system, and the initiation of legal measures in accordance with applicable legislation.

All API requests directed to BKT's Open Banking infrastructure go through a secure authentication and authorization protocol based on OAuth 2.0, where each call is tied to a valid token created through a multi-factor authentication (2FA) process.

BKT ensures the security and integrity of client data in accordance with personal data protection regulations, guaranteeing that processing is carried out only based on valid consent and for specified and proportionate purposes.

BKT declares that has taken measures to ensure that the dedicated API interface offers at all times the same level of availability and in cases the interface does not operate as intended will inform the applicant on the alternative options to recover the service.

BKT shall not be held responsible for delays in the execution of the payment order deriving from technical errors or misuse of the interface or systems of the applicant. In case of incidents the applicant should promptly notify the bank on the issue. Third parties accessing this service are not permitted to store, use, or process the data beyond the duration authorized by the client, and any excess of this period constitutes a breach of the terms and will result in immediate termination of access.

Use of the Open Banking service does not exclude or limit BKT's right to suspend, restrict, or temporarily terminate access in cases of suspected abuse, security risk, breach of agreement terms, or by order of competent authorities.

TPPs and users agree that all actions carried out through the Open Banking platform are recorded in secure logs and may be used by BKT for verification, audit, or legal compliance purposes.

The applicant declares that will be liable for any financial or reputational damage affecting the bank as a result of actions or negligence of the applicant.

The applicant agrees that any support or services from the bank not included in the API interface documentation or required from regulatory framework can be subject to applicable fees.

The applicant declares that will not use any of the data transferred or processed through the API interface other than for the purpose of the payment services.

The applicant agrees and declares that will inform the bank immediately in case of cyber security incidents affecting his systems or platforms that can pose a threat also to the API interface and will be liable to compensate the bank in case of failure to comply with the provisions of this paragraph.

The applicant agrees that the bank has the right to block access to the API interface or suspending or canceling a request for access at any moment when risk of fraud, unauthorized access or cybersecurity is identified by the bank. This document may be amended by BKT at any time, with prior notice and publication of the updated version on the developer portal or the bank's official website. Continued use of the service after the new version enters into force implies full acceptance of the revised terms.

Any dispute arising from the application of these terms and conditions shall first be resolved amicably; failing that, it shall fall under the jurisdiction of the Albanian courts, applying the current legislation of the Republic of Albania.

Interaction within the Use of the Developer Portal

The Developer Portal aims to establish an interaction channel to assess and verify the reasons for requesting access to specific functions of the platform, as well as to continuously improve the simulation experience in support of API development or other technical integrations. BKT reserves the right to contact you based on the information provided during registration, for the purposes of technical supervision, platform optimization, and portal usage management.

Key Responsibilities – Third-Party Provider

- The TPP is responsible for the accuracy and integrity of all payment instructions and customer data submitted to BKT Albania via the Open Banking API. This includes beneficiary account details, payment references, and any metadata associated with the transaction.
- The TPP must ensure that its platform complies with applicable regulatory and technical standards, including those defined under PSD2, Law no. 55/2020, and any security obligations outlined in BKT's Developer Portal Terms & Conditions.
- Any errors originating from the TPP's application—such as duplicate payment initiation, incorrect customer consent handling, or misrouting of payment parameters—are the sole responsibility of the TPP.
- The TPP is expected to maintain real-time monitoring mechanisms and logging tools to detect failed transactions, capture customer-side anomalies, and facilitate troubleshooting in collaboration with BKT Albania's technical teams.
- TPP holds responsibility for ensuring that the customer-facing environment (e.g., mobile/web interface) displays accurate and complete information prior to transaction confirmation, and that all user consents are captured in line with applicable legal frameworks.

Termination of Your Registration

Banka Kombëtare Tregtare reserves the right to terminate your registration and access to the Developer Portal and its related content at any time, without being required to provide prior notice. Your registration will be automatically terminated if you breach any of these Terms and Conditions. Upon termination, all rights granted to you under this document will be automatically revoked.

For any issues during the use of the service, the user or the applicant may contact BKT at the email address: openbanking@bkt.com.al or applicationsupport@bkt.com.al.