HELLENIC BANK

TERMS & CONDITIONS OF USE OF HELLENIC BANK DEVELOPER PORTAL AND API INTEGRATION

THESE TERMS AND CONDITIONS (the **Terms and Conditions**) are a contract between You (the **Developer**) and Hellenic Bank Public Company Ltd (the **Bank**) and must be read and applied in conjunction with any other agreements and/or terms and/or communications of any form between You and the Bank for accessing and/or registering to Developer Portal and/or relating to the Developer Portal and/or API process, except as otherwise expressly provided in these Terms and Conditions, or as the context of these Terms and Conditions otherwise requires. By registering and/or accessing the Developer Portal and/or integrating with the APIs in either the Sandbox or Live Environment, You agree to comply with and be bound by these Terms and Conditions. If You do not agree with these Terms and Conditions, please refrain from using the Developer Portal or APIs.

1. Definitions

1.1. **"Account"** means the Accounts, including Payment Accounts, held with the Bank and/or to be held with the Bank in the name of the account holder, who pursuant to the application and/or to a notification by the account holder to the Bank from time to time, shall be connected through the internet and/or telephone lines and/or via electronic and/or other connections as shall be determined or made available to its Customers by the Bank from time to time, with the Online Banking (for any account that the Online Banking is available);

1.2. **"Account Information Services (AIS)"** means services that provide access to account information held by Account Servicing Payment Service Providers (ASPSPs);

1.3. **"APIs"** mean application programming interfaces, made available by the Bank to allow the PSU access to and/or use of API Content/Services;

1.4. **"API Content"** means data and information made available by, and/or delivered through, a particular API;

1.5. **"API Content/Services"** means API Content and/or API Services associated with an API;

1.6. **"API Services"** means services and functions accessible through, and/or performed by, a particular API;

1.7. **"Business to Business (B2B)"** means a software application developed by a TPP, which enables legal entities, which may be Customers of the Bank, to interact with the Bank and offers to B2B Customer a comprehensive suite of financial services, including AIS, PIS, and CBPII;

1.8. **"Card Based Payment Instrument Issuer (CBPII)"** means the service that issues card-based payment instruments to Customers that include credit cards, debit cards, or other types of payment cards that enable PSUs to make electronic transactions and payments based on their explicit Consent;

1.9. **"Cardholder"** means both the main Cardholder as well as, where applicable, the authorised Cardholder who will be jointly and severally liable for all card transactions;

1.10. **"Client Application"** means a software application developed by TPPs that interact with the APIs to provide Payment Services or B2B;

1.11. **"Client Credentials"** means authentication Credentials (e.g. ID, secret) assigned to a Client Application and integrated with the Bank's systems through the Developer's Portal;

1.12. **"Consent"** means the PSU's consent/authorization granted to the TPP for providing Payment Services;

1.13. "**Customer**" means a natural or legal person who holds/maintains an Account with the Bank and/or is a Cardholder;

1.14. **"Developer Credentials"** means authentication information (e.g. username or identifier and a corresponding password, token, or other secure mechanism) unique to the TPP or Developer accessing the Developer's Portal;

1.15. **"Developer Data"** means information submitted by a TPP during the registration and integration process, including contact details, Client Credentials, and related metadata required for access to the Developer Portal and APIs;

1.16. **"Developer or You"** means the TPP or legal entities or the authorized, by such legal entities, third persons that facilitate B2B interactions, accessing the Developer Portal and integrating with the APIs;

1.17. **"Developer Portal"** means the designated online platform provided by the Bank, offering access to APIs, documentation, and tools necessary for TPPs to develop and integrate Client Applications for Payment Services or B2B;

1.18. **"Live Environment"** means the production platform designated for the execution of real electronic transactions related to Payment Services;

1.19. **"Payment Account"** means an Account which is used for the execution of Payment Transactions;

1.20. **"Payment Initiation Services (PIS)"** means services that enable the initiation of Payment Transactions at the request of the PSU through the API and subsequent transfer to the Bank;

1.21. **"Payment Services**" mean the AIS, CBPII, PIS;

1.22. **"Payment Services Law (PSL)**" means the Law on the Provision and Use of Payment Services and Access to Payment Systems of 2018, L. 31(I)/2018, in force at any given time;

1.23. **"Payment Service User (PSU)"** means a Customer of the Bank making use of a Payment Service in its capacity as payer, payee or both (as defined in PSL);

1.24. **"Payment Transaction"** means an action by the payer or on its behalf, or the beneficiary (as defined in PSL), which consists of a disposal, transfer or withdrawal of funds in relation to a Payment Account, regardless of any subjective obligation between the payer and the beneficiary;

1.25. **"PSU Credentials"** means the authentication information (e.g. a combination of a username, password, and additional security factors, such as one-time passwords or biometric authentication, ensuring secure access to their Accounts and transactions) specific to the PSU, used to verify their identity when accessing the Bank's services through a TPP's application;

1.26. **"PSU Data"** means the information related to the PSU, including account details, transaction history, and personal data, accessed and processed by the TPP through the APIs;

1.27. **"Regulatory Framework"** means the laws (primary and secondary) in force and/or applicable, at any given time, in the Republic of Cyprus, as well as any regulations, directives, regulatory policies, guidelines, rules and industry codes that are binding to the Bank, and/or to which the Bank is subject, and that apply in relation to and/or within the scope of these Terms and Conditions;

1.28. **"Requests Per Second (RPS)"** means a metric that quantifies the rate at which requests or transactions are made to an application, system, or service within a span of one second. In the context of these terms and conditions, RPS refers to the maximum number of incoming requests that a TPP is permitted to make to the APIs within a single second, as established by the Bank to ensure system stability and optimal performance in accordance with the Regulatory Framework and industry standards;

1.29. **"Sandbox Environment"** means a testing and development environment to enable TPPs to test their software and Client Applications used for experimenting with the APIs without conducting real transactions;

1.30. **"Strong Customer Authentication (SCA)"** means the verification, based on the use of two (2) or more details by the PSU during Payment Transactions through API Services, of the PSU's identity, or details by the Developer through Developer's Portal. Such verification can be achieved using such details via SMS, email, Mobile App (using biometrics only), DigiPIN and Soft OTP;

1.31. **"Third-Party Providers (TPPs)"** means the Payment Service providers providing Payment Services or B2B to the PSU;

1.32. **"Online Banking"** means the electronic banking services at any given time provided by the Bank and/or any company of the Group of the Bank, to Customers or authorised persons by such Customers who have access and/or use Online Banking, for the execution of financial and/or banking and other transactions and/or orders/instructions and/or the selection of banking and/or other products through ATMs and/or an electronic computer and/or via telephone communication through the Bank's Customer contact center and/or any other equipment required through the web and/or mobile phone or through such other electronic links and/or telephone and/or radio and/or television signals through which access to such services is or can be provided, as such may be determined by the Bank from time to time and which include, among other, the transfer of funds from and to an Account, electronic transfer of files, utility payments, orders for granting of cheque books, deposit forms and Account statements, providing information on exchange rates, creating standing orders information relating to cards granted by the Bank, revocation of cheque payments, information relating to hire purchase agreements and other services and/or facilities provided by the Bank, application for Account opening, issuance of non-plastic cards (temporary card numbers which can be used to make only one payment and which expire upon termination of the period of validity which the Customer or authorised person by such Customer who have access and/or use Online Banking determine) and other services as determined (or offered) by the Bank;

2. Registration of Developer

2.1. For registering to the Developer Portal and integrate with the APIs, the Developer is solely responsible for completing the registration process and providing accurate, complete, and up-to-date information to any relevant applications/documents. This information may include, inter alia, details about the Developer's identity, organization, and intended usage of the APIs.

2.2. The Developer is also solely responsible for protecting and maintaining the confidentiality of the Developer Credentials and of any activities occurring under the Developer's Account.

3. Registration of Client Applications

3.1. Upon successful registration of the Developer to the Developer Portal, the Developer has the right to create and register Client Applications.

3.2. The Developer is solely responsible for protecting and maintaining the confidentiality of the Developer's Credentials, including any Client Credentials associated with the Developer's registered Client Applications. Any activities carried out using the Developer's Credentials, shall be the sole responsibility of the Developer and not the Bank.

3.3. The Developer acknowledges that all actions taken under the Developer's registered Client Applications, whether in the Sandbox or Live Environment, are attributed to the Developer and the Developer alone, and the Bank shall not, in any circumstances, be held liable for any damages and/or losses and/or other consequences arising from such actions.

4. Registration and Usage of eIDAS Certificates

4.1. The Developers, excluding Developers who develop B2B, shall register and utilize electronic identification and trust services certificates, specifically qualified certificates for electronic seals and certificates for website authentication ("eIDAS certificates"), as part of the Developers' integration with the APIs.

4.2. Such Developers agree to provide accurate and up-to-date information regarding the eIDAS certificates registered on such Developers' Account, including relevant eIDAS certificate details and any related authentication mechanisms.

4.3. Such Developers are responsible for ensuring that the registered eIDAS certificates are valid, properly maintained, and compliant with the Regulatory Framework.

4.4. Upon submission of the eIDAS certificates, the Bank will take all reasonable measures required to ensure the authenticity and integrity of the eIDAS certificates and will notify such Developers whether such certificates have been accepted or rejected.

4.5. The Bank reserves the right to verify the validity and authenticity of registered eIDAS certificates and to request additional documentation or information to support such verification.

4.6. Any actions or transactions performed using eIDAS certificates registered on such Developer's' Account, are the sole responsibility of such Developers who shall be held liable for any damages and/or losses and/or other consequences resulting from such actions.

5. Registration and Usage of Mutually Authenticated Certificates

5.1. Developers who have developed B2Bs only, acknowledge and accept that they are responsible to register mutually authenticated certificates for their B2B Client Applications by submitting them to the Bank's designated system. Such Developers undertake to ensure that provided certificates must comply with industry standards and encryption protocols endorsed by the Bank and relevant competent authorities.

5.2. Upon submission of the certificates, the Bank will take all reasonable measures required to ensure the authenticity and integrity of the certificates and will notify such Developers whether such certificates have been accepted or rejected.

5.3. Such Developers are responsible for maintaining the validity of their mutually authenticated certificates, by, inter alia, proceeding with timely renewals and immediate update in the case of certificate expiration.

5.4. The Parties agree that registered mutually authenticated certificates must be exclusively used for the designated B2B for which they were registered.

5.5. Such Developers acknowledge and agree that they are prohibited from sharing, distributing, or using these certificates for any other purposes. It is provided that Developers shall ensure and confirm that B2Bs comply with the applicable registration requirements, data security standards and the Regulatory Framework.

5.6. The Bank reserves the right to audit and monitor the usage of registered certificates to ensure ongoing compliance with security measures. Any breach of security or misuse of such certificates by such Developers, may result in the suspension or termination of access to the Bank's systems or other appropriate remedies the Bank may seek.

6. Usage Rights of the Developer Portal

6.1. The Bank grants the Developers a limited, non-exclusive, non-transferable, and revocable right to access the Developer Portal and use the APIs solely for the purposes of providing Payment Services and/or B2B.

6.2. The Developers' usage rights are contingent upon adherence to Regulatory Framework. Usage by the Developers, of the Developer Portal beyond the scope of Payment Services and/or B2B, or any usage that violates the provisions of the Regulatory Framework, is strictly prohibited and may result in termination of the Developer's access.

6.3. The Developer may not resell, distribute, or otherwise commercialize the APIs or any related materials. The Developer is prohibited from reverse-engineering, decompiling, or attempting to extract the source code of the APIs.

6.4. The Developer shall:

(i) ensure compliance with SCA requirements, maintain secure communication channels when accessing and utilizing the APIs and the Payment Services and/or B2B and ensure the confidentiality, integrity, and authenticity of the PSU Data exchanged;

(ii) promptly report to the Bank any incidents, vulnerabilities, or breaches that may affect the security, integrity, or availability of electronic transactions or PSU Data;

(iii) implement necessary measures to monitor and detect any unusual or suspicious transactions and safeguard PSU Data in all transactions;

(iv) comply with the Regulatory Framework;

(v) cooperate with competent authorities, including relevant supervisory authorities.

7. Access Limitations and Usage Quotas

7.1. When Developers are granted the right to initiate an unlimited number of unattended daily accesses to Payment Accounts' information and PIS, in accordance with the Regulatory Framework, TPPs are responsible for ensuring they are compliant with SCA requirements and safeguard the integrity and confidentiality of PSU Data. In relation to attended access by the Developers, where the PSU actively requests such access process, it is provided that such access remains unrestricted in accordance with the Regulatory Framework.

7.2. The Bank reserves the right to monitor and review the usage of attended and unattended daily accesses. Developers are required to promptly report any unusual or suspicious activities to the Bank, as outlined in the security and data privacy requirements.

8. RPS and Response Limitations

8.1. Developers are required to adhere to the RPS when interacting with the APIs, monitor and manage their request rate by implementing appropriate mechanisms to regulate their outgoing requests and ensure that their activities remain within the defined limits.

8.2. In the event that the established upper limit of RPS is breached, the Bank reserves the right to temporarily withhold responses to incoming requests. This measure is implemented to prevent system overload and to maintain the quality of service for all PSUs.

8.3. If a breach of the RPS occurs, Developers shall be promptly notified by the Bank through established communication channels. Developers are required to take immediate corrective actions to mitigate the breach and prevent its recurrence. It is provided that the Bank reserves the right to temporarily withhold responses to incoming requests.

9. Sandbox Environment

9.1. The Developers acknowledge and accept that:

(i) any data submitted to and transactions performed within the Sandbox Environment, are for testing purposes only and do not involve real financial transactions;

(ii) no sensitive information shall be shared through the Sandbox Environment;

(iii) outputs or results obtained from such actions should not be interpreted as actual financial outcomes or results;

(iv) It shall not to use the Sandbox Environment to conduct transactions with real financial value or to engage in any activity that could simulate or interfere with real financial operations.

10. Live Environment

10.1. Utilization of the Live Environment for Payment Services and/or B2B, by Developers is subject to compliance with the Regulatory Framework which encompasses the secure access and retrieval of Account information and/or the initiation of Payment Transactions with the explicit PSU's Consent.

10.2. Prior to transitioning to the Live Environment, the Developers are responsible for securing the necessary authorizations, licenses, and certifications mandated by the provisions of the Regulatory Framework and the Bank.

10.3. Developers must ensure the security, confidentiality, and integrity of any electronic Payment Transactions performed by them within the Live Environment.

11. API Usage

11.1. The Developers warrant that they shall use the APIs solely for the purposes of developing and testing Client Applications.

11.2. The Developers acknowledge and accept that they shall not use the APIs for any illegal, unauthorized, or harmful activities, including but not limited to any fraud, data breaches, or malicious hacking.

11.3. Under no circumstances is the Bank to be held liable in the event of fraud, intent, or negligence by the Developers.

12. Security and Data Privacy

12.1. The Developers are responsible for implementing appropriate security measures to protect PSU Data obtained through API usage, including but not limited to data exchanged through eIDAS certificates.

12.2. The Developers shall implement security measures that ensure the confidentiality, integrity, authenticity, and non-repudiation of electronic Payment Transactions and PSU Data exchanged using the APIs and eIDAS certificates.

12.3. The Developers must comply with the Regulatory Framework, when handling PSU Data and eIDAS certificates related information. This includes obtaining necessary Consents from the PSUs for the processing of their PSU Data and ensuring proper encryption and security mechanisms for data transmission and storage.

12.4. The Developers agree to promptly notify the Bank of any data breaches or security incidents that may impact the confidentiality or integrity of PSU Data or eIDAS certificates related information. The Developers shall take appropriate remedial actions and cooperate with the Bank in addressing such incidents.

13. Consent Validity and Expiration

13.1. The Consent is required before initiating any transactions or accessing the Payment Accounts' information.

13.2. The validity period of the Consent shall be determined in accordance with the provisions of the Regulatory Framework.

13.3. Upon the expiration of the Consent validity period, the Developers are required to cease any Payment Services and/or B2B.

13.4. If the PSU intends to continue utilizing Payment Services and/or B2B beyond the expiration of their Consent, the Developer are obligated to obtain a new explicit Consent.

13.5. The Developer shall provide Users with timely notifications before their Consent expires, informing them of the impending expiration and the steps required to renew their Consent.

13.6. In compliance with the PSU's rights, the Developers are obligated to offer explicit functionality that allows the PSUs to revoke their Consent at any time. This revocation should be easily accessible through the Developer's platform or services.

13.7. The Developers are responsible for ensuring that their activities adhere to the rules and requirements related to Consent's validity, expiration, and revocation.

14. Support, Communication, and Incident Reporting

14.1. The Bank shall provide appropriate support channels to assist the Developers in addressing issues, queries, and technical concerns related to the APIs and their integration. These support channels may include online resources, documentation, and designated points of contact.

14.2. The Developers are required to report any incidents or vulnerabilities related to the APIs or their integration that could compromise the security, integrity, or availability of electronic Payment Transactions. Incidents include but are not limited to unauthorized access, data breaches, system failures, and any other security events.

14.3. The Developers shall promptly notify the Bank of any incidents or vulnerabilities the Developers discover while using the APIs or any associated systems. Such notifications should include detailed information about the incident, its impact, and any mitigating actions taken.

14.4. The Developers shall collaborate with the Bank to address and resolve reported incidents and vulnerabilities in a timely manner. Depending on the nature and severity of the incident, the Bank may request additional information or documentation to facilitate its investigation and response.

14.5. Communication between the Developers and the Bank regarding incidents, vulnerabilities, and support matters shall be conducted through the designated communication channels established by the Bank. This may include email, ticketing systems, or other secure means of communication.

14.6. The Bank shall maintain records of incident reports and our responses in compliance with the Regulatory Framework.

15. Changes and Updates to the APIs and/or these Terms and Conditions

15.1. The Bank may introduce changes, enhancements, updates, or modifications to the APIs, the Developer Portal, and/or these Terms and Conditions.

15.2. In line with our commitment to transparency and communication, the Bank shall provide the Developers with reasonable notice of any planned material changes to the APIs and/or these Terms and Conditions. This notice shall be communicated through the Developer Portal, email, or other established communication channels.

15.3. The Developers are responsible for regularly reviewing these notices to stay informed about any changes or updates that may impact the Developer's API integration, usage, or obligations. By continuing to use the APIs, after the amended Terms and Conditions coming into force, it means that the Developers have accepted the amended Terms and Conditions.

15.4. The Bank shall make diligent efforts to minimize disruptions to the Developer's API integration during changes and updates. However, it's important to acknowledge that temporary unavailability, interruptions, or impacts may occur as a result of changes to the APIs or associated systems.

16. Intellectual Property

16.1. The Bank exclusively retains all intellectual and other property rights in all procedures, functionalities, software, and documentation accessible in the Developer's portal. The intellectual and other property rights may not be modified, copied, altered, reproduced, adapted, or translated without the prior express Consent of the Bank.

16.2. The Developers acknowledge and accept that all the Bank's intellectual and other property rights are a substantial investment by and of substantial value to the Bank, governed by the Regulatory Framework. In the event of an actual or threatened breach of these Terms and Conditions that would diminish or impair such investment and value, the Bank will be entitled to an injunction order and/or other legal actions against the Developer and such measure will be in addition and without prejudice to any other rights and/or remedies that the Bank may have.

16.3. Any Client Applications, software, or content developed by the Developer using the APIs remain the Developer's property, subject to the rights granted to the Bank for the purpose of providing the APIs.

17. Indemnification

17.1. The Developers undertake to and will indemnify and hold harmless the Bank and any of its affiliates, officers, directors, employees, agents, successors, and assigns, for any losses, liabilities, penalties, fines (civil, criminal or administrative), or damages (including reasonable attorney's fees and expenses), that may result from:

(i) non- compliance with these Terms and Conditions and/or

(ii) any operating instructions given by the Bank and/or

(iii) any fraud, intent, wilful misconduct or negligence by the Developers and/or

(iv) any use of Client Applications and/or access to and/or use of the Developer Portal, any APIs and/or API Content/Services in a manner that does not correspond to these Terms and Conditions.

18. Limitation of Liability

18.1. Subject to the provisions of the Regulatory Framework, the Bank will not be, nor be held, liable, in any way to any person, for any claims, losses, damages, penalties or fines (civil, criminal or administrative), of whatever nature including without limitation any direct, indirect, general, special, punitive, incidental or consequential damages or other losses of any kind or character, even if such losses or damages , or may have arisen out of or in connection with the access to and/or use of the Developer's Portal, any API(s), and/or API Content/Services.

19. Termination

19.1. The Developers may terminate these Terms and Conditions by providing written notice to the Bank. Upon termination, the Developers' access to the APIs and API Services will be revoked, and the Developers will no longer be able to initiate electronic Payment Transactions or initiate and/or use any services stipulated in these Terms and Conditions.

19.2. The Bank reserves the right to terminate these Terms and Conditions (with immediate effect) under the following circumstances:

(i) if any of the Developers fail to comply with these Terms and Conditions;

(ii) if any of the Developers are found to be in violation of the Regulatory Framework and/or any regulatory requirements, licenses, or eIDAS certifications;

(iii) if the use of the APIs and/or API Services, from any of the Developers, results to a data breach, security incident, or any unauthorized access to PSU's information;

(iv) if the Bank determines that any of the Developers' activities do not align with the provisions of SCA and/or secure communication.

19.3. The Bank may terminate these Terms and Conditions at its absolute discretion by giving prior two (2) months' notice.

19.4. Upon termination of these Terms and Conditions, the following will apply:

(i) the Developer will no longer have access to the Developer Portal, APIs and any related services provided by the Bank;

(ii) any Developer Data, PSU Data, or transaction records associated with the Developers' Account may be retained or deleted in accordance with the Bank's data retention policies; and

(iii) the termination of access shall not release the Developers from any of their obligations, liabilities, or indemnities that have accrued before or at the time of termination.

20. Data Processing

20.1. The Parties will process any personal data in accordance with the Regulatory Framework, including the EU Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation).

20.2. Without prejudice to clause 20.1. above, any personal data provided to the Bank by applying for, and through, access to and use of the Developer's portal, APIs, and API Content/Services, will be used to: (i) provide and manage the Developers Account; (ii) track, extract, compile, aggregate, archive and analyze any behavior relating to access to and/or use of the Developer's portal, APIs, and/or API Content/Services.

20.3. The Bank disclaims all responsibility and liability and will not be responsible, nor be held liable, in any way to any person (including the Developer and/or any PSU) for or in relation to any processing of data by Client Application.

20.4. The Bank retains ownership of all ancillary information and metadata related to access to and/or use of the Developer's portal, the APIs, and/or API Content/Services, including, but not limited to listing appearance frequency and popularity of Users (Metadata). Metadata will be considered confidential information of the Bank.

21. Anti-bribery and Anti-corruption

21.1. The Developers where and as appropriate, undertake to:

(i) comply with the Regulatory Framework relating to anti-bribery and anti-corruption and will not engage in any activity, practice or conduct which would constitute bribery, extortion or solicitation;

(ii) adopt and implement adequate and appropriate policies and procedures for the prevention of bribery and corruption, including (but not limited to) training of any employees;

(iii) promptly report to the Bank any request or demand for any undue financial or other advantage of any kind, received by them in the context of and/or relating to the Developer's Portal, any API(s), and/or API Content/Services, and/or any activity, practice or conduct, which constitutes or would constitute bribery, extortion or solicitation in connection with the Developer's Portal, any API(s), and/or API Content/Services and

(iv) comply with the Bank's Anti-Bribery & Corruption Policy, including (but not limited to) the anti-bribery and anti-corruption programme thereunder, the Code of Business Conduct & Ethics, and the Conduct Risk Policy, as these are reflected through the Hellenic's Bank website.

22. Miscellaneous

22.1. These Terms and Conditions constitute the entire agreement between the Developer and the Bank regarding the registration to, access to and use of the Developer Portal and integration with the and use of APIs.

22.2. No waiver of any provision of these terms shall be deemed a further or continuing waiver of such provision.

23. Severability

23.1. The invalidity of any provision of these Terms and Conditions shall not affect the validity of any other provision of these Terms and Conditions. In case one or more provisions of these Terms and Conditions are invalid or become invalid as a result of any changing legislation, the validity of the remaining.

24. Governing Law

These Terms and Conditions shall be governed by and construed in accordance with the laws of the Republic of Cyprus and shall be subject to the jurisdiction of Cyprus Courts.