Terms and conditions for the use of digital banking service

1. Introduction

The Terms and Conditions for Use of Digital Banking (hereinafter referred to as "***Terms and Conditions")*** regulate the rights and obligations of the Bank as the service provider and the ***Customer*** in relation to the contracting and use of digital services banking (hereinafter referred to as the "*Service*")..

2. Definitions

- **Bank** – Intesa Sanpaolo Bank Albania, with Headquarters in Rruga Ismail Qemali nr 27, Tirana, Albania,
  Website: www.intesasanpaolobank.al;
  Contact: tel: +355 4 2276000; 0800600 (free form Albtelecom and Eagle), +355 692080903;
  Banks' branches, whose list is available on the Bank's website www.intesasanpaolobank.al;
- **Customer** – refers to a Bank's customer who has at least an active account with the Bank (in which he is sole owner and/or joint holder with single rights to operate in the account) who requires using the Digital Service.
- **User** – refers to the Customer approved by the Bank to use the Digital Service
- **Remote Communication** - means that the Service can be used without the simultaneous physical presence of the User and the Bank for the purpose of access to and use of the digital banking service, including the conclusion of distance contracts: internet banking, mobile banking, and other means that the Bank will subsequently introduce.
- **The Digital Banking Service (Service)** - encompasses the possibility of contracting and using banking and financial services through means of remote communication, providing insights into account balance and transactions, enabling performing of payment transactions and enabling contracting of banking and financial services contracts in electronic form (where applicable).
- **Public part of the Services** - a part of the Services available to everyone, including some users services, without prior application. It contains information about getting to know the functionalities of the Service, the Currency Calculator and the Bank's exchange rate information, ATM list, Bank's contact details. For service users, it also provides in the Mobile Banking (widget), a quick overview of the status of the selected Account, the ability to initiate activation, and use certain Services functionality, and initiate a login using #withKEY authorization device. The Bank reserves the right to change this content.
- **Private Part of the Service** - part of the services available to Customers who have successfully accessed the service through Authentication / Authorization.
- **Authentication** - User identification procedure with personalized security elements (credentials). The authentication process allows verification of the use of a particular authentication / authorization system, including the verification of personalized security elements and thus verification of the identity of the User.
- **Authorization –** the process of granting consent to execute payment orders, conclude certain contracts or for any other purpose supported by the Service. By Authorization, the User of Services accepts the terms presented to him prior to authorization (whenever applicable). The options and manner of authorization depend on the characteristics of the Service and the behavioral analysis of the user.
- **Security elements** – means the secure elements used for either authentication or authorization including but not limited to SMS OTP (one time password), PIN code, #withkey (Software Token), or Hardware Token.
- **Registration code** – set of numbers required for activation of the mobile banking application, which consists of two parts - the identification code and the activation code provided by the Bank to the User via different channels, which may be SMS, Internet banking application or other channels defined by the Bank. The Bank may make available part of the registration code via call center and in the branch office.
- **Authentication / Authorization Systems** - devices, applications, or methods for authentication and authorization for access to and use of digital banking services:
  - **#withKEY** - authentication and authorization system integrated into the mobile banking application for access to and use of the Service. The credential for running this system is a PIN.
  - **Smart login** - authentication and authorization system integrated into the mobile banking application for access to and use of the internet banking application Services that are provided by sending a push notification, or by sending the SMS code. The user can choose to use the Smart login system when accessing the Service. Smart login system is also used to implement TDS authorization.
  - **Token -** a personalized physical device generating a onetime password accessible by PIN used to authenticate users and authorize transactions.
  - **User ID** - a unique identifier of the User when contracting the Service. It is used as one of the elements to verify the User's identity when accessing the Service.
  - **Biometric methods** - authentication and authorization methods based on the physical characteristics of the User (e.g. fingerprint, face identification). The Bank may, for the purpose of access and use of the Services, enable the user to authenticate and authorize biometric methods in accordance with the technical capabilities of the User and the Bank. For the purpose of using biometric authentication / authorization methods to access and use the Services, the Bank may use the personal information that the User has stored with a third party (within the software of the device used to access the

Service) and activated it for authentication / authorization within the Services (eg Fingerprint, Face ID), without storing them on the Bank's side, and does not collect, store and use the biometric parameters of the User with prior consent of the User.

- **Touch ID** - a method for authentication and authorization using a fingerprint of the User, which was previously stored in the software of his mobile device and supports the fingerprint reader and is subsequently activated in the mobile banking application.
- **Face ID -** method for authentication and authorization by identifying the face of the User, which was previously stored in the software of his mobile device that supports the Face Identification functionality and is subsequently activated in the mobile banking application.

The User can use biometric methods depending on the technological capabilities of the mobile device he uses.

- **#withSIGN** - Qualified Electronic Signature, for the purposes of these General Terms is considered to be a Qualified Electronic Signature based on a Qualified Certificate issued by Intesa Sanpaolo S.p.A as a Qualified Trusted Service Provider under a special contract. A signed Qualified Electronic Certificate is used to electronically sign the documentation when contracting banking and financial services through the Digital Service.
- **One Time Password (OTP) -** a set of numbers that are generated upon request though #withKEY or a physical token, with a time-limited duration, that can only be used once.
- **Transaction Data Signing** – means a secure authorization method for example in case the beneficiary account is not trusted, or the behavioral analysis shows there is need for a more secure means of authorization, etc.
  It is performed using the Smart login authentication / authorization system - as an authorization by sending an automatic Push message. In case it is impossible to use these procedures for technical reasons, it is sent as an SMS.
  - **Sending a push message** - a payment order authorization procedure in the digital service that takes place in such a way that the User through the internet banking application initiates the sending of the Push request to a mobile device number that has previously been registered in the Bank and has been used for contracting the Service. The notification contains some elements of the payment order (for e.g. Beneficiary, Amount and Code).
  - **SMS Authorization** - a payment order authorization procedure in the Digital Service that takes place in such a way that the Bank sends a SMS message to the User's Mobile Phone Number that has previously been registered in the Bank. The SMS message contains some payment order elements for e.g. Beneficiary, Amount and Code. .
- **Limit** – implies the maximum volume of certain payments ordered within a day (for daily limit) and within a calendar month (for monthly limit) which the customer is allowed to execute through the Digital Service.
- **Push Notifications** - Notifications sent by the Bank to the User on the mobile device, related to products, services and events the sending of which has previously been selected and activated by the User in the Settings section of the Service. The user decides whether or not to use the option to initiate the notification and accordingly selects each option to activate within the service.
- **#withPAY payment** - a functionality that allows customers to perform payments directly from the app pre-login page by selecting payment recipient from his native contact list. The payer, instead of the recipient's account number, uses for information previously associated with the particular recipient who has registered before in the payment community. The information that a User can link to his transaction account number for the purpose of implementing this type of transaction may be the mobile phone number or other information that the Bank may subsequently import. The user decides whether to use this functionality and accordingly provides the necessary data and consent to activate this functionality.
- **Easy Transfer** - the functionality enables the user to perform payments between his own products (accounts or accounts and bank cards in case of Cards Pay-off, etc) without authorization. The User decides whether to activate the option within the Service.
- **Trusted Account** - a functionality that enables payment transactions of money transfer through the digital banking service to the recipient's account that the User has entered into the Beneficiary list and labeled it as a trusted account without performing a transaction authorization procedure. The user decides whether to activate the option and authorizes it by entering a PIN or a one-time password.
- **Fast Balance** - functionality that allows you to inspect the current state and available amount of an account in the public area of the service. The user decides whether to use this functionality and, accordingly, select the option within the application and authorize it by entering a PIN or a one-time password. If the User wants to see the status and the available amount, he can do so in specific widget of the Mobile application.
- **Pay&Go** – is the cooperation between the Bank and Pay&Go shpk a company registered in Albania, which allows the Customer to make payments to selected Pay &Go Partners either at Bank's ATMs located in the territory of Albania or through their mobile/internet banking applications. Pay &Go Partners are the financial and/or commercial entities that have subscribed an affiliation agreement with Pay&Go for the payment of their invoices or bills through the Pay&Go payments platform.

3. Terms of Use of Digital Banking Services

The contract on the use of the Service can be concluded at the Bank's branches and through direct banking services or online public portal, when the Bank enables it.

Every customer with at least one opened current account is eligible to contract the digital banking service.

In the case of several account holders, the Bank shall only provide the service to each account holder only when each of the holders has the right to operate with the account/s independently (single signatures)– with the provision that the Bank concludes the Agreement for the service with each account holders which requests the service.
In the case of jointly held bank accounts, account holders with joint disposal rights are not eligible for using the digital banking service.

To use internet banking, the User is required to access the service from a personal desktop or laptop computer, tablet or other appropriate device (meeting technical conditions specified in the Bank's Internet Banking User Manual) and should be connected to the Internet. To use the mobile banking application, the mobile application needs to be downloaded from the specified stores and on a device meeting technical conditions specified in the ISPA Mobile Banking User Manual) and should be connected to the Internet.

4. Technical Conditions

When contracting the Service, the User is obliged to provide the Bank with the telephone number of the mobile device to which the Bank will provide part of the registration code (identification code) necessary for the activation of mobile banking application. The User should also provide the Bank with an e-mail address to which the Bank may provide documents related to the Service, if the need be.

The Customer shall ensure that the parameters of the browser are set appropriately, in accordance with the required technical conditions.
The Bank shall not be liable for any damages that result if the User did not use the devices, or software required for the digital banking service in the appropriate manner, that is, the Customer did not access and use the service from the sites or web stores specified in the manual but with the intermediation or assistance of another site or platform (software), or did not exercise appropriate care in selecting a suitably secure environment in which to use the digital banking service. The Bank is not liable for damage arising from virus contamination in the User's IT system.

The Bank shall accept no liability for any damages caused by the fact that the parameters of the browser are different from the required technical conditions.

5. Access and use of the service through the mobile banking application

Downloading the application
To access and use the Service through the Mobile Bank application, the User should use a mobile device compatible with technical requirements and using the identification method selected by the Customer and specified in the Agreement.

The user downloads the mobile banking application through the virtual store App Store or Google Play store, depending on the mobile platform it uses.

Registration
For first login into the mobile application, upon contracting the Services, the User shall download the Mobile Bank application and install it on its mobile device and perform the registration process by entering into the respective fields in mobile application the registration code required for the activation of the Mobile Banking Application: the code received from the Bank's branch office and the code received by SMS in the mobile phone number of the Customer.

After the installation and activation of the mobile application by a one-time entry of the registration code assigned to the User, the User defines the personalized security element – the PIN (as well as activates other biometric security elements such as fingerprint or face id or other biometric methods made available from time to time), which he will later use to access and use the mobile banking application. The PIN serves the User for Authentication when accessing the Service in mobile and might also be used when applicable to provide customer's consent to execute payment transactions, and product contracting or for any other purpose offered and supported within the Service, in accordance with the applicable regulations.

- If the User has chosen to use the PIN as consent to execute payment transactions and provide other consent, it is not necessary to authorize them using a biometric method.
- If the User has chosen to use Face ID for authentication and to grant consent for the execution of payment transactions and any other consent, it shall not be necessary to authorize them using another biometric method or PIN.
- If the User has chosen to use Face ID for authentication and to grant consent for the execution of payment transactions and any other consent, it shall not be necessary to authorize them using another biometric method or PIN.

Re-Registration
If the installed Mobile Banking application is locked, deleted or the User wants to install on another mobile device instead of the existing one, the new registration code (identification and activation code) is required to reactivate the application again. The new registration code for activating the mobile banking application can be requested by the Service user in branch or through Call center. Through the latter, only if successful identification is achieved.

The use of the authentication methods is in keeping with the procedures applied at the Bank for Customer identification and the verification of disposal rights over the bank account. Beyond this, the Bank does not examine the entitlement of a User to use the credentials in accordance with the above, or the circumstances of such use.
The Customer bears full liability in respect of all such banking transactions, and instances of use of supplementary services, as are initiated by the User with the application of one of the above identification methods made available to the User

6. Access and use of the Services through the Internet Banking application

To access and use the Services through the Internet Banking application, the User accesses the web site.

Access and use Services through the Internet Banking application are possible using one of the following - authentication / authorization systems:
#withKEY – If the customer has chosen the software token, he can log into Internet Banking only after the he has downloaded and registered the mobile application into which is embedded the #withkey which will generate the one time passwords for authentication and authorization if applicable. The user accesses the internet banking home screen and is authenticated by entering in the “User ID” field the User ID provided by the bank and by entering a one-time password generated by #withkey in the "One-time password" field of the internet banking.
Authorizing transactions and giving consent where required, is done by entering a one-time password generated by the #withKEY authorization system into the predicted field in internet banking. An exception to this procedure is the TDS authorizations, which are authorized using the smart login authorization system.
Hardware token - If the customer has chosen the hardware token, the user accesses the internet banking home screen and is authenticated by entering in the “User ID” field the User ID provided by the bank and by entering a one-time password generated by the Token.
Authorization is done by entering into the provided field in the Internet Banking a one-time password generated by a token. An exception to this procedure is the individual TDS authorization of the order.

7. User Rights, Obligations and responsibilities

User rights
With his electronic signature, the Customer may request additional, not yet used services or the modification of the used Services via the Bank’s Internet Banking or the Bank’s mobile application. The acceptance (confirmation) of the application by the Bank constitutes a conclusion of the Agreement or a modification of the original Agreement.

Through the Service the Customer will be able to access all products and services he has with the bank and which the bank has enabled to be viewed, contracted and closed through these channels.

User is obligated to:
- store devices and data for authentication and authorization so as to prevent their damage, destruction, loss, unavailability, theft or misuse
- not to record on paper, electronic or other media, nor to reveal or make available to third persons PINs, passwords, and other data necessary for access to and use of the Service
- use the authentication and authorization system in a way to preserve its secrecy: the password, PIN and data generated by the authentication / authorization system must not be written, disclosed or made available to third parties
- pay to the Bank in accordance with the Bank's Terms and Conditions, all relevant fees, if it loses or damages the token, or if he does not return it after the termination of the contract on the use of the digital banking service
- notify the Bank without delay of the loss, theft or misuse of the authentication / authorization device, or mobile device on which mobile banking application is installed or its unauthorized use, and the Bank will, upon receipt of notification, execute the blocking of the authentication / authorization device and / or service.

The security obligations of the User are as follows:

- to access the Service use the appropriate computer (hardware and software) and communication equipment that meets the criteria for using the Service and is in accordance with the recommended configuration published on the Bank's website and / or in the Bank's branches, and which has been installed and updated, in accordance with all the latest available upgrades by the manufacturer: operating system, Internet browser, antivirus protection and firewall

- comply with all security measures for the protection and use of computers, mobile devices and other devices that have activated the use of the service, including:
  - protect access to the computer, mobile and other devices with a confidential password
  - secrecy of the PIN to prevent unauthorized use
  - to take into account the websites that visit the devices accessing the Service because access to some sites involves an increased risk of infecting computers, mobile devices and other devices with malicious programs
  - regularly updating the antivirus program
  - access the Service only at indicated URL.
  - regular checking of new notifications sent by the Bank to the User through the service and acting in accordance with such notices
  - immediately inform the Bank about the change in the number of mobile telephone devices for the safe functioning of the service (SMS delivery for SMS authorization and SMS with the identification code necessary for activating mobile banking application)

8. Obligations and responsibilities of the Bank

Any successful access to the service, authorization made is deemed to have been made by the User. The Bank will regard the payment orders given using the above methods of identification as approved by the User, and will fulfill the instruction given with respect to a service specified in the User Manual using the above methods of identification as an instruction given by the User, and the agreement related to the service shall be established, amended or terminated through the confirmation of the instruction by the Bank. The Bank does not examine the entitlement of a user to use the User ID or the password, or the circumstances of use.

The Bank reserves the right to modify the range of services associated with the various digital service. The Customer may find detailed information on the range of services, on the way in which they may be used, and on the technical requirements, in the relevant User Manual or may be informed through the digital banking service or in the banks website.

The Bank shall not be liable for any damage to the User due to:

- malfunctioning or improper operation of computers, mobile or other devices that are not owned by the Bank and used to access the Service
- failure of the computer system or operating system of mobile devices used to access the Service
- the user or other unauthorized person's access to the assigned device and / or the authentication / authorization application
- force major under which war, disorder, terrorist activity, natural disaster, epidemic, strike, cessation of electricity supply, disturbances in telecommunications and other traffic, errors in the transmission of telecommunication networks, decisions and actions of government bodies, as well as all other similar circumstances whose occurrence cannot be attributed to the Bank or that are beyond the control of the Bank and which have prevented the use of the digital channel
- loss, damage or destruction of the User's data and equipment

9. Fees

When concluding a Service Agreement, the User is obligated to pay the relevant fees for the execution of a Payment Order through the Service, and other fees contained in the Terms and Conditions of the Bank for the duration of the Service Use Agreement.

Should the User not have sufficient funds available in the designated account, then the Bank has the right to retain the incurred charges/commissions from any other bank account/product the customer has in the bank.

The amount and types of fees and other costs that may be incurred through the performance of the Services Agreement are defined in the Bank’s Terms and Conditions.

10. Limits

To use the digital banking service, daily and monthly payment limits for payment transactions in national, international and cross-border payments are applied. Information on the amount of daily and monthly limits are available to the User in both Mobile Banking and Internet Banking Services.

The User may increase/decrease limits within the default value assigned by the Bank either via branch or via the digital banking service. The daily and / or monthly limit specified at the User's request is applied immediately.

When using the Daily and Monthly Service, payment transactions for foreign currency transactions are reduced to foreign currency equivalent, according to the buy exchange rate of the Bank.

The Bank determines which types of transactions do not affect the reduction of daily and monthly limits, namely:

- Transfer to myself (transfers between customer's own accounts in LEK)
- Currency conversion (transfers between customer's own accounts in other currency)
- Standing order
- Direct debits (customer can set their own limit during the time of direct debit setup)
- Card payoff (repayment of credit card dues)
- Sale of deposits
- Other transactions as may be enriched from time to time

11. Execution of Payment Transactions

The Bank through the Services enables the User to execute domestic and cross-border payment transactions when enabled. Payment orders authorized by the Service are executed in accordance with the information published in the Terms and Conditions.

Depending on the type of authentication system and authorization used by the User, the consent to execute a payment transaction is provided by the User through authentication / authorization systems in accordance with the methods described in this document.

The Bank allows the User through the service to activate the so-called Fast Transfers procedure. Once the User independently or via ISBA's Internet Banking Application Services chooses and authorizes the use of this functionality through the authentication / authorization system that he / she uses, when initiating payment orders, the system will not require the individual authorization of the order from the User. The user independently through the digital service may deactivate this functionality.

The Bank allows the Customer through the Service to determine the so-called trusted account, for which the system will not require the execution of authorization procedure. A trusted account can be any account in favor of which the User decides to initiate payment orders without undergoing the authorization process. The Customer may deactivate this functionality through the Digital Service.

The Bank allows the Customer to activate through the Service the #withPAY payment functionality.

The Bank will send to the Customer the statement of account/s and or other banking products which the Customer has with the Bank only through the digital banking platform whenever this option is enabled. Other alternative means of receiving the bank statements may be configured from the Customer himself in the digital banking service.

12. Operating hours of the Digital Service

The systems are available 24 hours a day except for the periodical closing and system maintenance periods. The bank shall inform the Customer about maintenance times accordingly.

During the regular maintenance of the Service, the User will be partially or completely disabled in using the Service. Regular Maintenance Services are performed at a time when, according to the Bank's estimate, is the lowest frequency of use of the Service.

The transaction timelines are as defined in the Bank's Terms and Conditions.

In the event of technical breakdown or malfunctions the bank shall commence work on correcting the fault within 1 Banking Day from the detection of the fault.

13. Change, restriction or suspension of the service

The Bank reserves the right to change, restrict or suspend the Service. The changing of the Service may especially, but not exclusively, take place in the event of a technological or interface-related upgrading or modernization of the Service, while a suspension may especially, but not exclusively, take place in the event of technical problems or serious malfunctions. The Bank shall notify the Customer through channel or any other means at its disposal not excluding in writing about the completion of the above. The Bank shall not be liable for any damage suffered by the Customer as a result of such change or suspension.

The Bank is entitled to restrict the Service for security reasons (security restriction) in the following instances:

- if in the interest of protecting Customers, (i) it is necessary for security reasons due to an attack on the Bank's system, or (ii) a suspicion of abuse involving the Service arises;
- if, in the Bank's judgment, there is reason to suspect that abuse, or unauthorized or fraudulent use, has taken place using the data relating to the identity of individual Customers (User ID, password, PIN code), which could affect several Customers

that cannot be precisely determined in advance, and in the Bank's judgment the suspension or the restriction is necessary in the interest of protecting the Customers; or
- in the event of a mass or targeted phishing attack, or the suspicion thereof.

The Bank shall notify the Customers of the start and end of the restriction on the Electronic Service, by simultaneously providing such information via the Service and displaying it in the Branches and on the website. The Bank shall not be held liable for any direct or indirect damage suffered by the Customer as a result of the security restriction.

14. Other provisions

These Terms and Conditions apply in conjunction with the Agreement on the Use of Digital Banking Service, and the Terms and Conditions of Intesa Sanpaolo Bank Albania. The Terms and Conditions are available at the Bank's branches and at www.intesasanpaolobank.al.

15. Privacy Policy

Intesa Sanpaolo Bank Albania, to better protect your bank account from the risk of fraud and/or identity theft, will analyze, anonymously, the data concerning your behavioral characteristics on the web and within the mobile banking App. This is done via third party provider (the "Third Party") that provides behavioral authentication and malware detection solutions to combat cybercrime, subsequently improving customer safety and security. This solution allows the Bank to enable the detection of anomalies in online banking sessions for fraud detection and prevention purposes.

In order to perform the analysis of the data concerning your behavioral characteristics, the third party will produce a pseudoanonymised profile that helps to confirm the genuine user behind the online banking session. A combination of behavioral factors is used to create the pseudoanonymized profile, without relying on personal identifiable information (PII), including, for instance, a) cognitive traits such as eye-hand coordination, device interaction patterns; b) physiological factors such as left/right handedness, press-size, hand tremors, arm size and muscle usage and c) contextual factors such as transaction, navigation, device and network patterns, hereinafter indicated as the "Data".

The Data are collected and processed by the Third Party for the purpose to protect the data subjects, during their online sessions, against cyber threats and fraudulent activity such as identity theft, fraud and malware.
The solution will be used in your interest as client; with the aim that you are not victims of fraud or to have someone else assume your identity.

Your Data is retained, for a period of time not exceeding that necessary to achieve the purposes for which it is processed, without prejudice to the retention terms required by law and/or in order to protect certain rights before the competent courts.
In particular, the Data collected by the Third Party, in order to create unique biometric profile, will be retained by this latter for the duration of the Customer's relationship with the Bank and use of the Banks's mobile app or online banking website as necessary to provide the Bank with the fraud prevention services.

To achieve the purpose indicated in the Section 1 above, the Bank shall communicate your Data to the Third Party in encrypted way using a hashed identifier, ensuring your security and confidentiality. The Data will only be used for the purposes of fraud prevention and will not be communicated to any other entities outside of the Third Party.

By signing this Terms and Conditions, the Customer authorizes the Bank to process Customer's personal data to the necessary extent and within the intended purpose, with Pay&Go and each of the Pay&Go Partners for performing the payment of Customer's invoices or bills through the Bank's ATMs located in the territory of Albania or through their mobile/internet banking applications.