BYLAWS OF PROVIDING THE MILLENET ONLINE BANKING SERVICE FOR CORPORATE BANKING CLIENTS AT BANK MILLENNIUM S.A.

CHAPTER I
General Provisions

§ 1.

"Bylaws of Providing the Millenet Online Banking Service for Corporate Banking Clients at Bank Millennium S.A.", hereinafter referred to as the Bylaws lay down the terms of providing the Millenet Online Banking Service at Bank Millennium S.A., hereinafter referred to as the "Bank".

§ 2.

1. The concepts used in the Bylaws denote:
   1) **Authorisation** – expression of consent by a User for the execution of a payment order or another operation in Millenet,
   2) **Secure Envelope** – an envelope containing a one-time, temporary code which is a Strong Authentication factor used to generate an Access Password during the first-time login process. The Code is valid 90 days from the moment of the assignment of the Secure Envelope to the User,
   3) **White List of VAT Taxpayers** – an electronic list of entities registered as VAT taxpayers, kept by the Head of National Revenue Administration under art. 96b of the Act on Tax on Goods and Services (VAT), made available on the website of the Ministry of Finance,
   4) **Biometric Module-Activated Data** – biometric data that a user of the Millenet Online Banking Service can store on his/her mobile device using the biometric module (e.g. hardware secure storage). Any access to Data activated using the biometric module requires the user to authenticate using the biometric module,
   5) **Biometric Data** – data which is a record of the individual characteristics of a Millenet Online Banking Service user, e.g. fingerprint, facial image,
   6) **Provider** – entity providing payment services on the basis of the Act, including the Bank and the service providers referred to in § 20,
   7) **Acceptance Group** – letter-defined (A, B, C, D, E, F, G) group denoting the possibilities of authorising financial and non-financial instructions by a User which are defined by the Client on the "Configuration of Authorisation Rules of the Millenet Online Banking Service for Enterprises" form,
   8) **Access Password** – password for logging on to the Millenet Online Banking Service,
   9) **One-Time P@ssword from the Hardware Token** – single-use six-digit password generated by the Hardware Token on the basis of the User's data input employed to authorise financial or non-financial instructions and for logging on to the Millenet Online Banking Service,
   10) **One-Time P@ssword from the Hardware Token with Reader** – one-time six-digit password generated by a Hardware Token with a reader on the basis of login data or the authorised transaction which the User sends to the device by means of scanning a graphic code containing the data, used for authorising a financial or non-financial instruction as well as logging on to the Millenet Online Banking Service,
   11) **Login SMS Password** – one-time digital password sent by the Bank to the mobile phone number defined by a Millenet Online Banking Service User employed for logging on to the Millenet Service as a logging security mechanism,
   12) **SMS P@ssword** – one-time digital password sent by the Bank to the mobile telephone number defined by a Millenet Online Banking Service User employed for authorising submitted financial or non-financial instructions and for logging on to the Millenet Online Banking Service,
   13) **Mobile P@ssword** – one-time password defined by the User in the Millenet system which is used for activating the Mobile Application or authorising orders placed via the Mobile Application,
   14) **Temporary Password** – one-time temporary four-digit code which is a Strong Authentication factor for generating an Access Password during the first-time login process. A temporary password is valid for 30 minutes from the moment of its generation and is set up by the User through contacting Helpdesk,
   15) **Helpdesk** – team that provides technical assistance regarding the Millenet Online Banking Service at 0801632632 and 225984031 on business days between 8:00 – 18:00, after these hours, client service being provided by the general-purpose telephone help lines of Bank Millennium S.A.,
   16) **Information about the Authorising User / Personal Data of the Millenet User** – form defined by the Bank, containing personal data of the Millenet User allowed to authorise orders which can contain the mobile phone number defined for SMS P@sswords,
   17) **Security Mechanisms** – solutions enabling a User to safely use the Millenet Online Banking Service, in particular: Millekod, login, Access Password, Login SMS P@ssword, Hardware Token, Hardware Token with Reader, TLS protocol, Mobile PIN,
   18) **Client** – resident or non-resident entity that has entered on to a Bank Account Agreement/Framework Agreement for Bank Accounts and Banking Services for Corporate Banking Clients or a Framework Agreement for the Maintenance of Term Deposit Accounts for Entrepreneurs who do not Have a Settlement Account with Bank Millennium S.A.
   19) **Users' Configuration** – the form "Configuring Users of the Millenet Corporate Banking Service", on which the Client applies for the setting up of Users, providing them with access to accounts, products and system functionalities; if the "transactional platform" option is selected on the form, the Users' Configuration form shall also be the "Users' List" in the meaning of the "Transactional Platform Availability Agreement", hereinafter called the Platform Agreement,
   20) **Users' Configuration for the Common Millekod** – form defined by the Bank on which Clients request the setting up of Users, providing them with access to accounts, products and system functionalities,
   21) **Configuration of Authorisation Rules** – the form "Configuration of Authorisation Rules for the Millenet Online Banking Service for Enterprises" defined by the Bank, on which rules for authorising payment orders and other operations in Millenet are defined,
   22) **Configuration of Authorisation Rules for the Common Millekod** – the form "Configuration of Authorisation Rules for the Millenet Online Banking Service for the Common Millekod" defined by the Bank, on which Clients define rules for authorising payment orders and other operations in Millenet for Common Millekod,
   23) **Biometric Logging** – the method of logging into the Mobile Application using the Biometric Identification Service,
   24) **Millekod** – Client ID number assigned by the Bank consisting of 8 digits which is employed by a Service User in order to log on to the Millenet Online Banking Service,
   25) **Common Millekod** – functionality in the Millenet Online Banking Service which permits using accounts belonging to different entities at the level of functionality of a single Millekod,
   26) **Millennium Leasing** – Millennium Leasing Sp. z o.o. with head office in Warsaw at ul. Stanisława Żaryna 2A (02-593 Warszawa), entered into the Register of Entrepreneurs of the National Court Register maintained by the Regional Court for the Capital City of Warsaw in Warsaw, KRS 13th Economic Division, under the number KRS 0000081821, with shareholders' equity of 48 195 000 PLN, REGON: 012015417, NIP: PL5260213126,
   27) **Biometric Module** – technical solution provided by the manufacturer of the mobile device and operating system that allows authentication of a User through biometric data,
   28) **Authorisation Tools** – technical solutions provided by the Bank (SMS P@ssword, one-time P@ssword from a Hardware Token, one-time P@ssword from a Hardware Token with Reader or Mobile P@ssword) for authorising Payment Transactions ordered by a User, administrative actions mentioned in § 14, instructions connected with ordering products or services as well as other orders and statements placed with the Bank,
   29) **Authentication Tools** – Bank-provided technical solutions, (Temporary Password, SMS P@ssword, one-time P@ssword from a Hardware Token or a Hardware Token with Reader, Biometric Identification Service) employed depending on the message transferred by the Bank in the Millenet Online Banking Service for Strong Authentication and Authentication,
   30) **Mobile PIN** – four-digit identification number used for logging on to the "Bank Millennium for Companies" Mobile Application,
   31) **PIN for a Hardware Token** – four-digit access code for a Hardware Token defined by a User before the first-time use of the device,
   32) **PIN for a Hardware Token with Reader** – four-to-eight-digit access code for a Hardware Token with Reader, defined by a User during the first-time use of the device,
   33) **Password Receipt Protocol** – the Bank's "Password Receipt Protocol" form, containing data identifying a user of the Millenet Online Banking Service and information identifying the Secure Envelope with the password for first-time logging issued to the user,
   34) **Protocol of Receipt of a Hardware Token/ Hardware Token with Reader** – Bank-defined "Protocol of Receipt of a Hardware Token with Reader" form containing the identification data of a Millenet Online Banking Service User and information identifying the electronic device issued to the User with keyboard and display or the electronic device with keyboard, display and reader,
   35) **Bank Account** – settlement account or term deposit account run by the Bank for the Client or account for deposit or loan settlements,
   36) **Payment Account** – account kept for a Client and used for performing Payment Transactions, the concept of payment account also including a bank account if such account is used for performing payment transactions as construed by the Act,
   37) **Authorisation Rules** – Client-defined on the form "Configuration of the Authorisation Rules" combination of simultaneous authorisations made by persons from specific acceptance groups required for authorising individual types of instructions,
   38) **GDPR** – Regulation (EU) 2016/679 of the European Parliament and of the Council 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 and repealing Directive 95/46/EC (General Data Protection Regulation),
   39) **eBOK Millennium Leasing Service** – internet module of the Clients Service System available on the Millennium Leasing website: www.millenniumleasing.pl. It is also available for the Users of the Millenet Online Banking Service who have satisfied the conditions set out in § 18 of the Bylaws. Using the eBOK service in the Millenet environment by a Client involves the Bank's access to information resulting from the conclusion and performance of a lease agreement, provided by Millennium Leasing in this service for the purpose of their presentation in the system,
   40) **Session** – access to the Millenet Service established with the use of Security Mechanisms,
   41) **Strong Authentication** – means Authentication ensuring the protection of data confidentiality based on the application of at least two factors that belong to the categories:
      a) knowledge (something only the User knows),
      b) possession (something only the User has),
      c) User's characteristics (something that characterises the User),

      which are an integral part of this authentication and are independent in the sense that the violation of

one of them does not undermine the credibility of the others,

42) **Hardware Token** – electronic device with a keyboard and display, generating on the basis of the User's data input one-time passwords (OTP) used for authorising submitted financial and non-financial instructions and for logging on to the Millenet Online Banking Service,
43) **Hardware Token with Reader** – electronic device with a keyboard, display and reader generating digital one-time passwords (OTP) on the basis of data of logging or of the authorised transaction, which the User sends to the device by means of scanning a graphic code containing the data,
44) **Payment Transaction** – deposit, transfer or withdrawal of cash initiated by payer or recipient (as construed by the Act),
45) **User Changes Authorisation Right** – authorisation to approve in keeping with the Authorisation Rules the activities performed under the Edit Users Right,
46) **User Editing Right** – authorisation to add, modify and delete a User directly in Millenet online banking,
47) **Agreement** – agreement concluded between the Bank and the Client on the basis of which the Bank provides the Millenet Online Banking Service,
48) **Millenet Online Banking Service** – service of remote access to products and services offered by the Bank, which is made available to a Client on the basis of a separate agreement enabling the making of declarations of will and knowledge The Millenet Online Banking Service includes:
   a) Millenet for Companies – enabling access to banking services via electronic systems, functioning at the Internet address indicated by the Bank,
   b) Mobile Application – "Bank Millennium for Companies" application enabling access to banking services via the Client's mobile device meeting the technical requirements defined by the Bank and published on the Bank's website,
49) **Biometric Identification Service** – service that allows to verify the identity of a User of the Millenet Online Banking Service on the basis of Biometric Data provided on a mobile device by the manufacturer of the mobile device or of the operating system installed on that device,
50) **Act** – Act of 19 August 2011 on Payment Services (as later amended),
51) **Authentication** – procedure allowing the Bank to verify User identity,
52) **User** – User of the Millenet Online Banking Service, natural person who uses the Millenet Online Banking Service to perform activities to which the User has been authorised by the Client (however Clients who are sole traders or partners in civil-law companies may be simultaneously users of the Millenet Online Banking Service), holding the login and Access Password and using Millekod, SMS P@ssword, Hardware Token, Hardware Token with Reader or Mobile P@ssword,
53) **Request to Set Up a Common Millekod** – form defined by the Bank used by the Clients for a Common Millekod to be set up.

2. The concepts not defined in the Bylaws have the meaning assigned to them in the "General Terms and Conditions of Opening and Maintaining Bank Accounts for Corporate Banking Clients in Bank Millennium S.A.," hereinafter referred to as the "General Terms and Conditions".
3. The Bank may give to offered products and services commercial names specified in the price list.

CHAPTER II
Conditions of providing and using the Millenet Online Banking Service

§ 3.

1. The condition of obtaining access to the Millenet Online Banking Service is:
   1) to sign a "Framework Agreement for Bank Accounts and Banking Services for Corporate Banking Clients" or an "Agreement for Providing the Millenet Bank Account Service" or a "Framework Agreement for the Maintenance of Term Deposit Accounts for Entrepreneurs who do not Have a Settlement Account with Bank Millennium S.A.",
   2) to submit at the Bank by the Client:
      a) Users' Configuration,
      b) Information on the Authorising User,
      c) copy of the personal identity card of each User (if required),
      d) Configuration of Authorisation Rules.
2. The Bank defines the scope of services available in the Millenet Online Banking Service.
3. The Millenet Online Banking Service is provided 24 hours a day, 7 days a week, reserving section 4.
4. The Bank may temporarily cease to provide the Millenet Online Banking Service in connection with the necessity to conduct necessary maintenance works or for security reasons. In the event that it is necessary to temporarily suspend the provision of the Millenet Online Banking Service due to the necessary maintenance works, the Bank shall inform the Client about the planned unavailability of the Service and the duration of the downtime in an appropriate message visible before logging on to the Service.
5. Millenet provides the Client with access to information delivered by the Bank for a period suitable for preparing such information and its manner of recording allows to retrieve it in unchanged form. A Client may record and store information and Communiques on an own durable data carrier.

§ 4.

1. Millekod, login, Access Password, SMS P@ssword, code from the Hardware Token or Hardware Token with Reader used for logging in and Mobile PIN or Biometric Identification Service in the case of the Mobile Application authenticate a User in the Millenet Online Banking Service and permit using the system in accordance with rights held.
2. In Users' Configuration the Client defines a login for every User, Authentication Tools and Transaction Authorisation Tools, i.e.:
   1) a Hardware Token or Hardware Token with Reader for generating authorisation codes and/or
   2) number of the mobile phone to which the SMSP@ssword for logging in, Access Passwords for the subsequent instances of logging as well as SMS passwords for authorising transactions will be sent by Bank.
3. The Bank submits to the Client the Millekod number through contacting over the phone one of the persons identified on the form – Users' Configuration.
4. Every User shall define his/her own Access Password with the use of Strong Authentication during the first-time logging process.
5. Users who have confirmed the receipt of the Hardware Token or Hardware Token with Reader on the Hardware Token/Hardware Token with Reader Receipt Protocol may use it upon the Bank's approval of such Protocol.
6. A User entitled to use the Mobile Application, after logging on to the Millenet Online Banking Service
   1) has the possibility to define an own eight-digit Mobile P@ssword,
   2) is given the right to set up/change his/her own Mobile PIN number.
7. The Mobile Application allows authentication using the Biometric Identification Service.
8. The user may enable or disable the use of the Biometric Identification Service in the settings of the mobile application.
9. Users must protect access to their mobile devices. The acquisition or use by third parties of Data activated using the biometric module may result in such persons obtaining unauthorised access to the Mobile Application.
10. The manufacturer of the mobile device or the operating system on that device shall be liable for the operation and security of the biometric module providing access to the Biometric Data activated using this module, unless this is a legal responsibility of another entity.
11. The Bank reserves the right to exclude the processing of the Data activated using the biometric module for security reasons or due to significant changes in the way the data activated with the biometry module operates or the inability to apply financial security measures in accordance with the requirements of the Anti-Money Laundering and Financing of Terrorism Act.
12. The defined mobile phone number to which SMS P@sswords are sent for logging in is also the number for contacting the User.
13. Entering incorrectly:
   1) an Access Password, P@ssword, Login SMS, Mobile PIN may cause their blocking, of which the User shall be notified prior to such blocking,
   2) an SMS P@ssword or Mobile P@ssword may cause the possibility of placing selected instructions to be blocked, of which the User shall be notified prior to such blocking.
14. Entering incorrectly a Hardware Token Code or Hardware Token with Reader Code, in successive attempts, may cause Access to the Millenet Online Banking System to be blocked, of which the User shall be notified prior to such blocking. In such case the Client, exercising the rights referred to in § 14 section 1, may unlock the User's access.
15. If none of the Users holds the rights referred to in § 14 section 1, the Client shall contact the Helpdesk or the Relationship Manager to the unlock the access.
16. Entering a Mobile PIN code incorrectly in successive attempts may cause the access to the Mobile Application to be blocked, of which the User shall be notified prior to such blocking. The access may be unlocked by entering the Mobile PUK code, which is available in Millenet.
17. Entering the PIN for the Hardware Token incorrectly three times in successive attempts triggers the unlocking process by showing on its display the code that should be entered upon logging on to the Millenet Online Banking Service. If the Hardware Token is a tool used for logging on to the Millenet Online Banking Service, the Helpdesk should be contacted.
18. Entering the PIN code for the Hardware Token with Reader incorrectly three times triggers the need to perform the unlocking process by means of scanning the graphic code available after logging on to the Millenet Online Banking Service. If the Hardware Token with Reader is a tool used for logging on to the Millenet Online Banking Service, the Helpdesk should be contacted
19. Entering a one-time password (OTP) generated by a Hardware Token or Hardware Token with Reader incorrectly three times makes it impossible to authorise using this device.
20. Entering the one-time password (OTP) provided in a Secure Envelope incorrectly three times in successive attempts shall result in blocking the possibility to use the code to set up an Access Password.
21. Entering a one-time Temporary Password incorrectly three times in successive attempts shall result in blocking the possibility to use the code to set up an Access Password.
22. If Authorisation Tools or Authentication Tools are locked, the Client should promptly contact the Helpdesk or the Relationship Manager to have them unlocked or replaced.

§ 5.

1. Access to the "Millennium Forex Trader" Service, to the extent stipulated in a separate agreement within the framework of the Millenet Online Banking Service shall be granted to Clients who have signed the Platform Agreement.
2. Access to the "Millennium Forex Trader" Service may be granted in writing only after submitting to the Bank the Users' configuration form.
3. Security mechanisms for logging on to the Millenet Online Banking Service by a User identified on the Users' Configuration form as person authorised to make transactions through the transactional platform constitute "Means of Authorisation" in the meaning of the Bylaws for the Provision of Telecommunications Services by Millennium Telecommunication Services sp. z o.o. This means that the a/m User's logging on to the Millenet Online Banking Service is equivalent to logging on to the Millennium Forex Trader Transactional Platform.

§ 6.

1. Access to the Millenet Online Banking Service is possible provided that the hardware and software used by the Client has been configured in keeping with the Bank's recommendations, in particular in keeping with the "Millenet Online Banking Service Manual," which is available on the Bank's website.
2. Technical requirements concerning devices which may be used to run the Mobile Application in the Millenet Online Banking Service are available on the Bank's website.
3. The Client is required to use the software version indicated by the Bank in the current version of the Manual referred to in section 1.

§ 7.

1. Users should use Security Mechanisms, Authentication Tools and Authorisation Tools appropriate for the Millenet Online Banking Service in a manner ensuring the observance of their confidentiality and are obliged not to make them available to other persons.

2. If there are suspicions that unauthorised persons may know Security Mechanisms, Authentication Tools or have access to Authorisation Tools, the Client should immediately:
   1) change them or block the Millenet Online Banking Service and then
   2) contact the Helpdesk or the Relationship Manager in order to obtain new Security Mechanisms, Authentication Tools or Authorisation Tools.

§ 8.

1. Personal data of the Authorising User must be confirmed by this Authorising User on the form – Authorising User Information / Personal Data of a Millenet User.
2. A User's personal data, including the mobile phone number used to receive login SMS P@sswords must be given by the Client on the Users' Configuration form.
3. The Bank does not permit using the same mobile phone numbers by different Users under one Millekod.
4. The Receipt of a Hardware Token or Hardware Token with Reader by a Millenet User entitled to authorisation must be confirmed with a protocol.
5. The Receipt of a Secure Envelope must be confirmed with a Secure Envelope Receipt Protocol. The Bank may issue a Secure Envelope personally to the User identified in the request or to a person authorised to make financial commitments on the Client's behalf whose specimen signature is on the Signature Specimen Card submitted to the Client's account.
6. Personal data of Authorising Users set up by the Client in the Millenet system must be confirmed on the form – Personal Data of a Millenet User. A User acquires authorization rights after a positive verification of the personal data by the Bank.
7. The Bank reserves the right for verifying the validity of Authorisation Tools used to perform an authorisation at any moment prior to executing a particular Payment Transaction or other instruction in Millenet. In the event of a negative verification the orders shall not be executed.
8. Setting up a Mobile P@ssword requires confirmation with an Authorisation or Authentication Tool.
9. The Bank in agreement with the Client may allow the employment of other Authorisation Tools than those referred to in § 2 section 1 item 9.

§ 9.

1. As part of the Millenet Online Banking Service the Client may grant Users rights concerning trade finance transactions. Access to trade finance services may be granted in writing only after submitting to the Bank the Users' Configuration form and the Configuration of Authorisation Rules form.
2. In granting rights to documentary letters of credit the Client authorises a User to place with the Bank orders to issue, change, transfer a documentary letter of credit; instruction to waive restrictions to documents; rejection of non-compliant documents presented under a documentary letter of credit; adding confirmation to a letter of credit; correcting or supplementing the text of the mentioned orders/instructions as well as performing other factual or legal actions connected with the processing of letters of credit.
3. In granting rights to bank guarantees the Client authorises the User to place with the Bank orders to issue, change a guarantee, reguarantee, Civil Law surety, aval, decision in principle to grant a guarantee or surety as well as perform other factual or legal actions connected with the processing of such products.

§ 10.

1. As part of providing the Millenet Online Banking Service a Client may apply for linking his or her accounts to the Millekod of another entity subject to its consent, under the Common Millekod function. The linking results in the possibility of granting access to accounts by Users of other entities who signed an "Application for Setting Up a Common Millekod" and performed the configuration of Users under a Common Millekod with respect to the newly added accounts of a different entity (Users' configuration for a Common Millekod as well as Configuration of Authorisation Rules for a Common Millekod).
2. Functionality rights granted to a User under a Common Millekod are valid for all entities assigned to this Millekod.
3. Changes regarding modifying, adding and deleting Users, rights and accepting orders and operations in Millenet as part of the Common Millekod functionality are performed by the Bank upon instructions from the Client submitted on a bank form or using an appropriate function in the Millenet service by the authorised User/Users.
4. An authorised User is understood to mean a person/persons holding the right to "edit users" and "authorise user changes".
5. Fees and commissions connected with access to the Millenet Online Banking Service, with Authorisation Tools etc. are collected from the Client's account to whose Millekod there have been linked accounts of other entities in the amount which corresponds to the Price List for Corporate Banking Clients.

CHAPTER III
Conveying Instructions

§ 11.

1. Users perform authorisations in accordance with their rights and the principles defined by the Client in the "Configuration of Authorisation Rules" document.
2. Strong User authentication is required, if the User gets access to his/her account online, initiates an electronic Payment Transaction, conducts through a remote channel an action that may imply a risk of fraud related to the performed payment services or other fraud as well as in case of services initiated by the Providers referred to in § 20. Each of the Authentication Tools used in the Strong Authentication mechanism must be set up and linked to a User.
3. Authorisation is made by confirming an instruction with a proper system function and an Authorisation Tool assigned to the User, i.e.:
   1) entering the SMS P@ssword received on the mobile phone number provided earlier,
   2) entering the one-time digital password generated by the Hardware Token,
   3) entering the one-time digital password generated by the Hardware Token with Reader,
   4) entering the Mobile P@ssword.

§ 12.

1. In order to ensure the security of funds on a bank account the Bank reserves the right to apply additional security procedures, such as for example confirming ordered payment instructions by contacting the telephone numbers indicated by the Client.
2. The daily transactions' limit in the amount of PLN 150,000 (or its equivalent in foreign exchange) is applied to instructions authorised by a single person with an SMSP@ssword and Mobile P@ssword.
3. The Bank may execute transactions exceeding the daily limit referred to in item 2, if the Client orders a Payment transaction to the recipient account to which he ordered Payment transactions earlier or after additional telephone verification with a person with powers to authorise in the Millenet system.
4. The Bank has the right not to execute a Payment Transaction order if it is impossible to obtain the confirmation of a submitted transaction for any reason.
5. The Bank has the right to block access to the Millenet Online Banking Service:
   1) in the event of the Service being used contrary to the provisions of the Agreement with respect to using the Millenet Online Banking Service,
   2) suspicion of using the Millenet Online Banking Service by unauthorised persons,
   3) in cases of suspicion or actual occurrence of any unauthorised transactions.
6. Promptly after blocking the access to Millenet or to the Mobile Application the Bank shall contact the Client or User to clarify the situation.

§ 13.

1. Orders and statements made and authorised by the User by means of the Millenet Online Banking Service within the duration of an established Session are considered as meeting the requirements of written form and result in the obligations and rights whose content is specified in communiques provided in the Millenet system.
2. The Client shall be liable for using the Millenet Online Banking Service also by the Users, including for the orders placed through it.
3. The Client is obliged to control the state of implementation of instructions placed by means of the Millenet Online Banking Service.
4. The content of an instruction placed in the mode specified in item 1 shall be legally binding on all the parties until the execution of the action.
5. Each ordering of a product or Service of the Bank placed by means of the Millenet Online Banking Service takes place upon prior acceptance by the Client of the conditions of using a given banking product or Service.

§ 14.

1. The administrative rights available in the Millenet Service, subject to § 10 section 3, enable in particular:
   1) setting up new Users and granting to them rights to accounts and operations,
   2) granting to Users with a blocked Access Password the statuses which permit unlocking their access,
   3) granting to particular Millenet Users the rights to accounts and operations,
   4) defining acceptance groups of Users of the Millenet Online Banking Service necessary to authorise specific types of Payment Transactions and other instructions in the Millenet system,
   5) enabling other Users of the Millenet Online Banking Service to activate the Mobile Application.
2. In the case of a Client's granting authorisation rights to a User of the Millenet Online Banking Service the provisions of § 10 shall apply.
3. The right to authorise a change of authorisation rules in the Millenet system may be granted to a User only by the Bank on the basis of written instructions submitted on a Users' Configuration form.

§ 15.

Payment Transaction orders placed during a Session debit the Client's bank account.

§ 16.

1. In the event of abandoning the performance of an operation in the Millenet system the Session shall be automatically terminated when the period of inactivity exceeds the limit defined in the system.
2. In case of abandoning the performance of operations in the Millenet system, in particular ceasing to submit instructions during the Session, the use of the Millenet Online Banking Service should be terminated by logging out.
3. A new Session must be set up to resume the use of the Millenet Online Banking Service.

§ 17.

1. When using the functions available in the Millenet service, authorised Users may submit to the Bank the following items, required by the Bank for Client Service:
   1) documents / information prepared by the Client as:
      a) scans of the original documents,
      b) unsigned information concerning the Client,
      c) documents in electronic form, bearing an appropriate qualified electronic signature,
   2) documents prepared by third parties / persons other than the Client, as scans of the original documents or documents in electronic form, bearing an appropriate qualified electronic signature.
2. A qualified electronic signature executed on the documents submitted to the Bank should satisfy the following conditions:
   a) A qualified signature should be issued by a qualified provider entered in the register of trust service providers kept by the National Bank of Poland or another provider located in the territory of the European Union, who is on the European Union Trusted Lists (EUTL),
   b) The certificate should be up-to-date, non-revoked, not cancelled at the time of executing the signature on the document.

§ 18.

1. As part of their access to the Millenet Online Banking Service Clients have the possibility of getting access to the eBOK Millennium Leasing Service.

2. The terms and conditions of providing the eBOK Millennium Leasing Service by Millenium Leasing Sp. z o.o. are specified by "Bylaws on the Provision of eBOK Millennium Leasing Sp. z o.o. service," hereinafter called "eBOK Bylaws".
3. Granting rights to the eBOK Millennium Leasing Service in Users' Configuration is equivalent to submitting a users configuration form in Millennium Leasing in accordance with the eBOK Bylaws.

§ 19.

1. In the Millenet Online Banking Service the Bank provides the service of White List of VAT Taxpayers verification i.e. an automatic check whether the account to which a payment is being made is on the White List of VAT Taxpayers.
2. The White List of VAT Taxpayers Verification Service is performed by the Bank upon the client's demand.
3. The Bank performs the verification with observance of the highest technological and security standards. Because the service is auxiliary with respect to the Millenet Online Banking Service and verification of the White List of VAT Taxpayers is made with the use of data provided by the Ministry of Finance, the Bank shall not be liable for inconsistencies of the verification result which will arise in result of errors or obsolescence in the data made available by the Ministry of Finance.

CHAPTER IV
Provider-initiated services

§ 20.

1. The User may use the following services initiated by the Providers:
   1) Payment Initiation Service (PIS) – means a service that consists in initiating a payment order by a Provider upon a User's request from a Payment Account kept by the Bank. The service includes information about initiating and conducting a Payment Transaction, which is the same as information made available to a User if the User initiates a transaction directly,
   2) Account Information Service (AIS) – means an online service that consists in providing to a User or a Provider consolidated information about at least one Payment Account kept for a Client by the Bank.
      The service provides information on a Payment Account and history of payment transactions, similar to the information presented in Millenet Service,
   3) The Service of Confirmation of the Availability of Funds (CAF) on a Payment Account – means an online service that consists in initiating, upon the request of the Provider issuing a card-based payment instrument, the Bank's confirmation of the availability on the Client's Payment Account of the amount necessary to perform a particular Payment Transaction executed on the basis of this card. Confirmation of the Availability of Funds does not mean their blocking on the Payment Account.
      Confirmation of the Availability of Funds on a Payment Account is not applicable to Payment Transactions initiated through card-based payment instruments on which electronic money is stored.
2. Services referred to in section 1 are available for Payment Accounts in PLN and foreign currency.
3. Services of the Providers are available for Users of Payment Accounts available online and require the use of Security Mechanisms available in the Millenet Online Banking Service.

§ 21.

1. The Bank executes services initiated by the Providers exclusively based on consents granted by the Users to the Providers or in the case of the service indicated in § 20 section 1 item 3 – to the Bank and exclusively within the limits of such consents.
2. The set of consents on the basis of which the services of the Providers are rendered and the data of the Providers are made available to the User in the consent repository in Millenet.
3. The set of rights enabling a User to consent to the provision of Provider-initiated services is defined in the Users' Configuration form.
4. The Bank, on the basis of the information supplied by the Providers about the explicit consent of the User, enables the Service Providers to perform services in the area of the Payment Initiation Service and the Account Information Service, based on Strong User Authentication applied in the relationship between the Client and the Bank.
5. In connection with the implementation of the Providers' services, Authentication Tools and Authorisation Tools are applied defined for the Millenet Online Banking Service.
6. Subject to section 7, the User may, through the Millenet Online Banking Service, withdraw the consent granted to the Bank and referred to in section 1 and may file an objection to the consents expressed to the Providers with immediate effect. Any withdrawal of the above consent means that every instruction received from the Provider after the withdrawal of the consent shall be rejected by the Bank.
7. In case of a Payment Initiation Service with current date, the User must not cancel the transaction after the Provider has been given consent for its initiation.
8. Every time, before the execution of an instruction the Bank verifies whether the Provider holds proper authorisations defined in the Act.
9. In order to execute a one-off Payment Initiation Service and one-off Account Information Service, the Bank presents the User with a summary of the information submitted by the Provider about the consents granted by the User and parameters of the requested service. Service implementation is approved with the use of Authorisation Tools available in the Millenet Service and in accordance with § 11 section 1.
10. In the case of a multiple account information service, upon receiving such order, the Bank, before the first-time execution of the service, presents the User with a summary of the information about the granted consent, submitted by the Provider, and the parameters of the requested service. Service implementation may be approved with use of Authorisation Tools available in the Millenet Service, and in accordance with § 11 section 1.
11. In the case of the service of confirming the availability of funds on the Payment Account, the User grants to the Bank a proper consent. Service implementation is approved with use of Authorisation Tools available in the Millenet Service, and in accordance with § 11 section 1.
12. The Bank may refuse to execute a Provider's service for reasonable reasons related to a suspected unauthorised action of the Provider.
13. The Bank shall inform the User about the refusal referred to in section 12 and its causes. Such information, if possible, shall be communicated to the User before access refusal, but no later than on the business day following the day of such refusal, unless the submission of the information is not advisable due to security reasons or is in breach of the law.
14. In the case referred to in section 12 the Bank enables the Provider to render the services immediately after discontinuing the causes justifying the refusal.
15. The Payment Initiation Service is provided within the daily transaction limit set by the User.
16. The Bank does not collect any additional fees for Provider-initiated services, while Payment Orders are executed by the Bank in accordance with the principles defined in the General Terms and Conditions and the price list.

CHAPTER V
Bank account statements

§ 22.

1. As part of the Millenet Online Banking Service the Bank provides the Client with the possibility of downloading bank statements.
2. The Client performs the configuration and establishes the frequency of generating the statements.
3. Configurations of certain types of statements may be made only by the Bank upon a Client's request.

CHAPTER VI
Scope of the Bank's Liability

§ 23.

As part of providing the Millenet Online Banking Service the Bank shall be responsible for the timely and content-compliant execution of Client' instructions, reserving § 25.

§ 24.

The Bank undertakes to observe banking secrecy to with respect to any information obtained from the Client in connection with the Millenet Online Banking Service.

§ 25.

1. As part of the Millenet Online Banking Service the Bank shall not be responsible for losses caused due to the circumstances beyond the Bank's control, i.e. for:
   1) force majeure – including e.g. natural disasters, riots, warfare,
   2) strikes,
   3) decisions of public administration bodies,
   4) suspension of the Millenet Online Banking Service for reasons beyond the Bank's control,
   5) submission of an instruction which does not comply with the applicable legal provisions,
   6) the Authorisation Tools and Authentication Tools being disclosed to unauthorised persons,
   7) provision of access to Security Mechanisms to unauthorised persons

   and in other cases where the Bank cannot be held liable under the law.
2. The Bank shall not be responsible for errors resulting from software other than the one supplied by the Bank.
3. The Bank shall not be liable:
   1) for the content of an instruction submitted by the Client received at the Bank as part of the Millenet Online Banking Service,
   2) for the malfunction of the installed equipment and the computer network used by the User,
   3) due to the use by the user of the Millenet Online Banking Service of browsers other than those recommended by the Bank,
   4) for Client computer's inadequate security:
      a) due to the failure to update the operating system,
      b) due to lack of antivirus software,
   5) for disclosing security mechanisms or authorisation tools to third parties,
   6) for damages caused by software not provided by the Bank,
   7) for lack of access to the Mobile Application resulting from the inability to transfer data via such Application.

CHAPTER VII
Scope of the Client's Liability

§ 26.

The Client shall be liable for the consequences of the Bank's execution of all orders and instructions if they have been executed in accordance with their contents.

§ 27.

The Client shall be fully liable for any acts and omissions of the Users of the Millenet Online Banking Service.

§ 28.

1. The Client must inform the Users about the conditions of the Agreement necessary to execute instructions as part of the Millenet Online Banking Service.
2. The Client shall be responsible for the proper use and observance of the rules of security and confidentiality of identifiers and passwords for the Millenet Online Banking Service and the Authorisation Tools in use.
3. The Client shall also promptly inform the Bank about any and all circumstances in result of which his Security Mechanisms, Authorisation Tools and Authentication Tools may have been used by unauthorised persons.

CHAPTER VIII
Millenet Online Banking Service Fees and Commissions

§ 29.

The Bank shall charge fees and commissions for the Millenet Online Banking Service, in amount and on the terms specified in the price list.

CHAPTER IX
Procedure and conditions for cancelling the Millenet Online Banking Service

§ 30.

1. The agreement for the provision of the Millenet Online Banking Service may be terminated in

writing by each of the parties, with a notice period of 30 days or by agreement of the parties at any time.

2. The Agreement regarding the Millenet Online Banking Service shall be terminated with the closure of the last settlement account / account for settlement of deposits in zlotys, held for the Client.
3. The termination of the Agreement for the provision of the Millenet Online Banking Service shall not result in the loss of access to the eBOK Millennium Leasing Service.
4. The procedure and conditions for cancelling the service of access to the eBOK Millennium Leasing Service are set out in detail in the eBOK Bylaws.
5. Cancellation of access to the eBOK Service does not mean termination of the Agreement on the provision of the Millenet Online Banking Service.
6. In matters relating to the procedure and conditions of termination of the Agreement not regulated in the Bylaws, the provisions of the General Terms and Conditions shall apply.

§ 31.

The Bank has the right to terminate the Agreement for important reasons which depending on the terminated scope of Agreement include:

1) sharing the Millekod, login, Access Password, Authorisation Tools or Authentication Tools with others,
2) reasonable suspicion of the Client's commission of an offence,
3) disclosure of inconsistencies with the factual status of information in the documents provided to the Bank and personal data,
4) lack of funds on the account for a continuous period of 3 months for the coverage of the fees and commissions due the Bank,
5) violation of the terms of the Agreement or the provisions of the Bylaws,
6) using the Millenet Online Banking Service contrary to its purpose.

CHAPTER X
Personal data

§ 32.

1. The User's personal data obtained by the Bank in connection with the provision of services set out in the Bylaws will be processed by the Bank, in accordance with the provisions of the GDPR, in order to:
   1) provide the services set out in the Bylaws, pursuant to Article 6 section 1 letter b of the GDPR as well as
   2) run activities carried out on the basis of separately granted consents, pursuant to Article 6 section 1 letter a of the GDPR,
   3) to carry out necessary legal obligations pursuant to Article 6 section 1 letter c of the GDPR,
   4) for purposes carried out under the so-called legitimate interests of the Bank as an administrator, including the performance of any activities in order to prepare for the conclusion, execution or termination of an agreement to which you are not a party (e.g. you have been appointed as a proxy, you are a representative or other person indicated by the Bank's Client), as well as to perform other legal activities related to the agreement, and furthermore to ensure the security of transactions, to prevent fraud, to carry out communications, and if necessary to investigate and defend against claims, on the basis of Article 6 section 1 letter f of the GDPR.
2. Personal data obtained within the Account Information Service, processed by the Bank for the purpose of providing the services specified in the Bylaws, will be processed by the Bank until the withdrawal of consent to provide the Account Information Service, unless the processing of personal data is necessary for the purpose of realisation of the Bank's legally justified interests, as an administrator of personal data, in particular for the establishment, investigation and defence of claims, on the basis of Art. 6 section 1 letter f GDPR, in accordance with the principles set out in the "Information on the processing of personal data at Bank Millennium S.A.".
3. A user has the right to request from the Bank access to personal data, their correction, deletion or restriction of processing, the right to object to processing, as well as the right to data transfer. To the extent that the basis for processing is an expressed consent, a User has the right to withdraw it, without affecting the legality of the processing that was carried out on the basis of the consent before its withdrawal. You have the right to lodge a complaint with a supervisory authority, i.e. the President of the Office for Personal Data Protection.
4. The principles of personal data processing are indicated in the document: "Information on the processing of personal data in Bank Millennium S.A.", available on the Bank's website in the Data Protection – Bank Millennium section.
5. With regard to the processing of personal data for the purpose of providing the eBOK service, the controller of personal data is Millennium Telecommunication Services sp. z o.o. The rules for the processing of personal data of Millennium Telecommunication Services sp. z o.o. can be found on https://www.millennium-leasing.pl/ochrona-danych.
6. With regard to the processing of personal data for the purpose of providing the "Millennium Forex Trader" service, the controller of personal data is Millennium Telecommunication Services sp. z o.o. The rules for the processing of personal data of Millennium Telecommunication Services sp. z o.o. can be found on the website: Millennium Telecommunication Services – Bank Millennium.

CHAPTER XI
Final Provisions

§ 33.

1. The procedure and rules for submitting complaints by Clients and their considering by the Bank are specified in the General Terms and Conditions.
2. To the extent not regulated in the Bylaws, the provisions of the General Terms and Conditions as well as generally binding legal regulations shall apply.

Warsaw, 30 October 2023