AS "PNB Banka", reg. No. 40003072918
15-2 Elizabetes street, Riga, Latvia, LV-1010
Phone: (+371) 67041100, fax: (+371) 67041111
e-mail: info@pnbbanka.eu, www.pnbbanka.eu

PROVISIONS FOR REMOTE SERVICES

Table of Contents

1. Terms and Abbreviations Used

1.1. **Remote Service** – a service that enables the Client to access the Account remotely, including to receive information about Accounts and/or handle the money in Accounts, to conclude agreements (submit applications) for the reception of Services, to submit applications, instructions to the Bank and carry out other activities the Bank offers by means of the automated systems of the Bank: PNB Internetbanka, PNB Vision, PNB SMS-Banka, infoLINE, PNB Chat, PNB Trade.

1.2. **User of the Remote Service** – the Client and/or the person authorised by the Client according to the procedure established by the Bank to use the Remote Services by providing such a person with the Electronic Identification Data and Authorisation Elements of the Client.

1.3. **Authentication** – the identification procedure, as a result of which based on the Electronic Identification Data the Bank may be reasonably sure that the Remote Service by means of the System is used by the User of the Remote Services.

1.4. **Bank** – AS "PNB Banka", unified registration No. 40003072918, registered address: 15-2 Elizabetes Street, Riga, LV-1010; email address: info@pnbbanka.eu; website: www.pnbbanka.eu, the supervision of the Bank is carried out by the Financial and Capital Market Commission (1 Kungu Street, Riga, LV-1050; email address: fktk@fktk.lv).

1.5. **DigiPass** – an electronic device used to form the Authorisation Element and the Electronic Signature of the Client.

1.6. **PNB Internetbanka** – a System accessed from https://www.ib.pnbbanka.eu, through which the Client is provided with remote access to the Services defined by the Bank**.**

1.7. **infoLINE** – a System that ensures remote access to the Services determined by the Bank by means of telephone communication. The service is provided using telephone numbers +371 67 041 100 (in Riga) or (+ 7 495) 780 04 02 (in Moscow).

1.8. **Code Card** – a plastic card that contains a fixed number of six digit codes used to form the Authorisation Element and the Electronic Signature of the Client.

1.9. **Agreement** – the Agreement consists of the application submitted by the Client for receiving the Remote Service, GPT, including these Provisions, and the Rates & Fees.

1.10. **Mobile Application** – PNB Internetbanka in the form of a mobile application, if the Client already has access to PNB Internetbanka and a mobile phone or another device/devices with Android or iOS operating system and access to the Internet.

1.11. **PNB Chat** – a System that allows the Client to contact the Bank in real time using special software in a secure information environment.

1.12. **PNB Chat Password** – the password issued to the Client by the Bank that enables the Client to access PNB Chat.

1.13. **PNB SMS-Banka** – a System that allows the Client to receive information determined by the Bank on the Client's mobile phone in a short message (SMS).

1.14. **PNB Trade** – a System, which is a part of PNB Internetbanka and enables the Client to conclude currency purchase and sales transactions with the Bank.

1.15. **PNB Vision** – a System set up on the Client's computer and allowing the Client to access remotely the Services determined by the Bank.

1.16. **PNB Vision Password** – a password issued to the Client of the Bank that enables him/her to use PNB Vision.

1.17. **Provisions** – these "Provisions for Remote Services", which are Annex 3 to the Bank's "General Provisions for Transactions" (GPT).

1.18. **Access Code** – the password issued to the Bank's Client for access infoLINE.

1.19. **System(s)** – the automated system(s) of the Bank (PNB Internetbanka, PNB Vision, PNB SMS-Banka, infoLINE, PNB Chat, PNB Trade).

1.20. **SMS-PIN** – a unique sequence of symbols generated by the Bank and communicated to the Client in a short message (SMS) sent to the telephone number indicated by the Client and that is used for user's authorisation in PNB Internetbanka and to form the Electronic Signature of the Client.
1.21. **Google Authenticator** - an application type Authorization element that generates a unique 6 (six) digit code and which is used for authorization of user in PNB Internetbanka and to form the Customer's Electronic Signature.
1.22. **GPT** – "General Provisions for Transactions" approved by the Bank, which regulate the legal relationship between the Parties and apply to all Services.
1.23. If any terms or abbreviations are used in these Provisions which are not defined in this section of the Provisions, such terms or abbreviations shall be interpreted in accordance with the terms and abbreviations defined in the GPT.

2. General Provisions

2.1. The Bank collects the Commission Fee for the provision of the Remote Service from the Client according to the Rates & Fees.
2.2. The Client agrees to refrain from disclosing his/her Electronic Identification Data used for work with the Systems to any third parties, and from transferring Authorisation Elements issued by the Bank to any third parties.
2.3. The Client uses his own (those at the Client's disposal) devices (a personal computer, fixed telephone, mobile telephone etc.) with a connection to electronic means of communication (the Internet, a telephone line) for work with the Systems. The Bank bears no responsibility for the quality of devices and electronic means of communication used by the Client, the confidentiality and safety of information transferred using them or any disruptions in their operation.
2.4. Special Passwords, Electronic Signatures, Access Codes and other means of identification mentioned in these Provisions are used to identify the Client, when he/she tries to access the Systems and for working with them.
2.5. The Client submits a Payment Order to the Bank by means of the System to accomplish transactions with the money in the Account. All details required to complete the Payment must be provided in the Payment Order and it must be signed with the Electronic Signature.
2.6. The validity term of a Payment Order submitted to the Bank by means of the System is 10 (ten) calendar days from the day the Bank has received that particular Payment Order. If during that period the Account balance remains insufficient to complete the Payment Order and pay the Commission Fee, the Payment Order becomes invalid and the Bank has no obligation to complete it.
2.7. In addition to cases indicated in Clause 3.11 of GPT the Bank is entitled to refrain from completing Payment Orders, to refuse to accept the Client's applications, the Client's agreements about the provision of Services, as well as other applications and documents from the Client in the following instances:
2.7.1. the Bank is unable to identify the Client based on the entered Electronic Identification Data;
2.7.2. the Bank has a suspicion that third persons could have connected to the System;
2.7.3. the text is unclear or damaged due to faulty communications.
2.8. The Bank bears no responsibility for any consequences of exercising or refraining from exercising the Bank's rights mentioned in Clause 2.7 of these Provisions.
2.9. In addition to cases mentioned in Clause 2.7 of these Provisions the Bank does not complete Payment Orders, refuses to accept applications from the Client, the Client's agreements on the provision of Services or other applications and documents from the Client in cases mentioned in the Applicable Law, agreements concluded between the Bank and the Client, their Provisions and in other cases indicated in GPT.
2.10. Upon receiving a Payment Order the Bank is entitled to contact the Client repeatedly to verify the correctness of the Payment Order.
2.11. The Bank is entitled to introduce or change at its discretion Electronic Identification Data limits for outgoing transfers from the Account and determine or change the range of Services available by means of the Systems depending upon the Electronic Identification Data used.
2.12. The Client may determine limits for outgoing transfers from the Account according to the procedure set forth in these Provisions.
2.13. If the Client has objections against a Payment made from the Account by means of the System, he/she may submit a complaint to the Bank. If a Consumer fails to submit a complaint to the Bank within 13 (thirteen) months, or within 3 (three) months, if the Client is not a Consumer, from the day of completion of the Payment, the Bank is entitled to regard it as the Client's recognition of the correctness of the respective Payment.
2.14. The Client must inform the Bank immediately about any Unauthorised Payment made in the Account, as well as about any error or inaccuracy made by the Bank that has occurred as a part of the Account maintenance process.
2.15. The Bank registers (records) all activities and conversations that take place by means of the System, and such recordings may be used as proof for resolving a dispute between the Client and the Bank.
2.16. The Bank bears no responsibility for errors, delaying settlements, inconsistencies and other deficiencies that have occurred as a result of the Client providing erroneous or incomplete information at the time of submitting Payment Orders or other documents to the Bank through the System.
2.17. All information submitted through the System using the Electronic Identification Data of the Client is regarded by the Bank as documents with equal legal force to any documents with the Client's original signature. All inquiries, announcements and notices delivered to the Client through the System by the Bank have the same legal force as documents signed by the authorised person of the Bank.

2.18. The Client has the right to discontinue the use of the System at any moment by submitting a respective application to the Bank.
2.19. Upon receipt of the Client's application about discontinuing use of the System the Bank closes the Client's access to the System within 3 (three) Bank's business days.
2.20. If the Bank closes the last Account of the Client connected to the Systems in the cases indicated in GPT and the respective Provisions, the Client's access to the Systems is terminated automatically.
2.21. The Agreement is considered terminated after closing the Client's access to the System and full payment for Services according to the Rates & Fees.

3. Identification of the Client by Means of the Systems

3.1. The Client must identify himself/herself by entering (notifying) his/her Electronic Identification Data to access the Account by means of the System or carry out other activities available in the System.
3.2. The following are the Electronic Identification Data of the Client for accessing the System and the Account:
3.2.1. the Client's Code (CIF);
3.2.2. Access Codes and Passwords;
3.2.3. Authorisation Elements.
3.3. The Electronic Signature is used to approve documents (including Payment Orders) dispatched through the System.
3.4. The Bank issues/notifies to the Client one of the special Electronic Identification Data for creating the Electronic Signature and the Access Code. The Client may have several Authorisation Elements at his disposal simultaneously:
3.4.1. the Code Card;
3.4.2. DigiPass;
3.4.3. SMS-PIN;
3.4.4. Google Authenticator;
3.4.5. the Access Code.
3.5. For the purposes of these Provisions the mobile phone number registered with the Bank (notified to the Bank) by the Client for receiving SMS-PIN and mobile phone or other device that is used for Google Authenticator usage is also considered the Electronic Identification Data of the Client, taking into consideration, however, that Clauses 3.7, 3.8 and 3.13 of these Provisions, which apply to Authorisation Elements mentioned in Clauses 3.4.1-3.4.4 of these Provisions, do not apply to such a mobile phone (as a device).
3.6. The Client is aware that any third party may be able to access the Account (obtain information and/or perform transactions using the money in the Account, including loan funds) by means of the Electronic Identification Data of the Client mentioned in these Provisions. The Client has an obligation to keep secret and out of reach of third parties his/her Electronic Identification Data and Authorisation Elements (the Client's Code (CIF), Password, Code Card, Access Code, DigiPass, mobile phone, on which the phone number registered for receiving SMS-PIN is used or mobile phone or other device that us used for Google Authenticator usage). The Client must report to the Bank immediately, if any third parties have acquired the Client's Electronic Identification Data (even if the Client only suspects it), as well as about a loss, theft or other unlawful appropriation of devices used to form or receive it, or any incident of unauthorised use of the Electronic Identification Data. The Client may inform the Bank of the aforementioned also by the Bank's round-the-clock telephone line for Client reports: +(371) 67041100.
3.7. If the Client has notified the Bank of a loss of the Electronic Identification Data or of the fact that third parties have acquired knowledge of it (even if the Client just suspects it), the Electronic Identification Data are blocked, including the possibility to receive SMS-PIN, the possibility to use Google Authenticator from the mobile phone or other device about which the Bank has received information about loss, theft or other unlawful appropriation and access to PNB Chat System. The Bank issues/prepares new Authorisation Elements, Passwords for the Client, unlocks the possibility to receive SMS-PIN and restores access to the PNB Chat System (issues a new PNB Chat Password among other things) based on a written application from the Client un unlocks the possibility to use Google Authenticator, based on Clients call to the Bank's Call Center, after payment of the Bank's Commission Fee according to the Rates & Fees.
3.8. The Bank has the right to block the Electronic Identification Data, the Client's access to the Systems, the possibility for the Client to receive SMS-PIN and Google Authenticator from the mobile phone or other device on which application is installed, also in cases related to the safety of the Electronic Identification Data, a justified suspicion about unauthorised use of the Electronic Identification Data or its use for fraudulent purposes, or in cases the Electronic Identification Data is related to a loan and the risk that the Client will not be able to fulfil his/her payment obligations towards the Bank has increased substantially, as well as in cases the Bank has received information about the death of the Client (a natural person) or the death of the sole legal representative or the representative with the right to represent the Client together with other representatives of the Client (a legal person), or the death of the beneficial owner (according to provisions of the Law On the Prevention of Money Laundering and Terrorism Financing of the Republic of Latvia). If the Bank blocks the Electronic Identification Data in circumstances mentioned in this clause, it informs the Client, if possible, before the scheduled date of such actions or immediately thereafter, except for cases, when provision of such information could endanger objectively justified security concerns or is prohibited according to requirements of the Applicable Law. The Bank shall not be liable for the consequences of exercising or not exercising of the Bank's rights specified in this clause.

3.9. The Bank bears no responsibility for losses incurred by the Client as a result of a third party gaining access to the System, including, if the third party has used the Electronic Identification Data of the Client, except, when the Bank has failed to ensure a possibility for the Client to report to the Bank a loss, theft or other unlawful appropriation of the Electronic Identification Data at any time and the Client has not taken any illegal actions in that particular instance.

3.10. The Bank does not compensate to the Client losses up to EUR 150 (one hundred fifty euro), which have been incurred as a result of Unauthorised Payments due to a loss, theft or other unlawful appropriation of the Electronic Identification Data, or the fact that the Client had failed to ensure secure storage of personalised security elements and thus allowed for an opportunity for somebody to misappropriate the Electronic Identification Data. Provisions of this clause do not apply to losses incurred after the Client based on Clause 3.6 of these Provisions has informed the Bank about a disappearance, loss of the Electronic Identification Data or about third parties acquiring the Electronic Identification Data, except for cases, when the Client has acted in an unlawful manner himself/herself.

3.11. The Bank does not compensate losses to the Client incurred by the Client as a result of Unauthorised Payments, if the Client has acted in an unlawful manner or intentionally (deliberately), or as a result of gross negligence has allowed for use of the Electronic Identification Data, which is contrary to these Provisions, or has failed to fulfil the reporting duty provided for in Clause 3.6 of these Provisions.

3.12. The Bank is entitled, at its discretion and taking into consideration the nature of personalised security elements of the Electronic Identification Data, as well as the circumstances, in which they have been lost, stolen or otherwise unlawfully appropriated, and if the Client has not acted in an unlawful manner and it has also not been established that the Client has intentionally (deliberately) allowed for use of the Electronic Identification Data, which is contrary to these Provisions, or has intentionally (deliberately) failed to fulfil the reporting duty to the Bank according to Clause 3.6 of these Provisions, to reduce the extent of the Client's liability as set forth in Clauses 3.10 and 3.11 of these Provisions. The rights of the Bank set out in this clause are not considered a compulsory obligation of the Bank.

3.13. In cases mentioned in GPT the Client undertakes to return the Electronic Identification Data to the Bank upon the Bank's request.

3.14. Access to PNB Internetbanka is blocked after 5 (five) consecutive attempts to enter wrong Electronic Signature symbols or other Electronic Identification Data of the Client.

3.15. The Bank may allow several Clients to share a DigiPass, if they have submitted to the Bank an application on a standard form and all of them have the same beneficial owner or authorised person, or the Client is a member of a group of Clients recognised by the Bank as such. In that case based on the application received from the Clients the Bank may create a group of users, which allows for simultaneous access to accounts of all members of the group of users by means of one DigiPass.

3.16. The Client must submit a written (paper) application on a standard form to the Bank or send the form in digitally through PNB Internetbanka, if the Client has access to the System, if he/she wishes to receive SMS-PIN, and indicate (notify the Bank of) the mobile phone number, on which the option of dispatch and receipt of short messages (SMS) is enabled, and on which the Client would like to receive SMS-PIN. One Client may indicate no more than two different mobile phone numbers for receiving SMS-PIN.

3.17. The Bank does not verify, whether the number notified by the Client according to Clause 3.16 of these Provisions is registered with the Client's name (belongs to the Client). In compliance with provisions of Clause 3.6 of these Provisions the Client must independently ensure that SMS-PIN does not end up in the possession of third parties.

3.18. After fulfilling Clause 3.16 of these Provisions the Bank dispatches SMS-PIN to the Client each time the Client chooses SMS-PIN to access the System or form the Electronic Signature and indicates to which mobile phone number notified to the Bank earlier SMS-PIN should be sent at a given time. Each SMS-PIN can be used as the Client's Electronic Identification Data only on the day it has been received from the Bank and until the time indicated in the Bank's short message. If the deadline is missed and the received SMS-PIN has not been used, it becomes invalid, and the Client must initiate the procedure of obtaining a new SMS-PIN repeatedly.

3.19. SMS-PIN can be used only by the Client (its legal representative), who has unrestricted rights to manage the Account alone. Provisions of Section 4 of these Provisions do not apply to SMS-PIN.

3.20. The Client pays the Fee for using SMS-PIN in the respective amount to the Bank according to the Rates & Fees on the last day of each month until such time the Bank receives an application from the Client about termination of use of SMS-PIN.

3.21. The Client has the right to indicate to the Bank another mobile phone number at any time, to which SMS-PIN should be sent in the future, or to terminate further use of SMS-PIN with a 3 (three) Banking days prior notice to the Bank in the form of a respective application in paper form or electronically by means of PNB Internetbanka.

3.22. The Bank bears no responsibility, if the Client does not receive SMS-PIN due to the Client's mobile phone being outside the area of reception, switched off or malfunctioning.

3.23. If the Client uses the Code Card to form the Electronic Signature, he/she must choose the six-digit code requested by the Bank and submit it to the Bank by entering it into the System. The Bank verifies the correspondence of the notified (entered) six-digit code to information about that six-digit code at the Bank's disposal.

3.24. If the Client uses DigiPass to create the Electronic Signature, he/she according to DigiPass User Manual (available at the Bank's website on the Internet www.pnbbanka.eu or at the Bank's Client service centre) enters the signature parameters into the System and informs the Bank of the value of the Electronic Signature created using DigiPass.

3.25. If the Client uses SMS-PIN to create the Electronic Signature, he/she enters the combination of digits received from the Bank in the short message into the System. The Bank verifies the correspondence of the transferred (entered) number to information about that particular version of the number at the Bank's disposal.
3.26. To use Google Authenticator, the Client should download and install the application on the mobile phone or other device and connect Google Authenticator in PNB Internetbanka as a new identification device.
3.27. If PNB Vision Password is used to create the Electronic Signature in the PNB Vision System, the Client must enter that password in the PNB Vision System and the Electronic Signature is created based on it and the unique parameters of the PNB Vision System.

4. Determining Electronic Signature Authorisations of the Electronic Identification Data

4.1. The Client may request the Bank to set up any of his/her Electronic Identification Data to allow only viewing or full access rights.
4.2. If the Client has several DigiPass devices at his/her disposal, after completing an application on the Bank's standard form and payment of the Commission Fee he/she may assign one or several of the Electronic Identification Data the right to establish the extent of authorisations of other selected Electronic Identification Data by limiting:
4.2.1. the available types of banking transactions;
4.2.2. beneficiaries of payments;
4.2.3. access to Accounts.
4.3. The Client determines the extent of the Electronic Identification Data authorisations on his/her own by sending standard notifications to the Bank through PNB Internetbanka.
4.4. If the Client has several DigiPass devices at his/her disposal, after completing an application on the Bank's standard form and payment of the Commission Fee he/she may set different Electronic Signature authorisations for each DigiPass device.
4.5. The Client may choose and establish sole signatory authorisations for the Electronic Identification Data with regard to signing of documents addressed to the Bank or only joint signatory authorisations with one or several other Electronic Identification Data of the Client.
4.6. A Bank document signed using the Electronic Identification Data with sole signatory authorisations is accepted for completion immediately.
4.7. A Bank document signed using the Electronic Identification Data that has joint Electronic Signature authorisations with one other or with several Electronic Identification Data is saved in PNB Internetbanka and accepted for completion only after it has been signed by the Electronic Signature created using the Electronic Identification Data indicated in the Client's application.
4.8. The Bank bears no responsibility for losses incurred by the Client as a result of any disagreements among the Users of the Client's Electronic Identification Data.

5. Use of PNB Internetbanka

5.1. PNB Internetbanka enables the Client to manage money in Accounts through the Internet, submitting electronic Payment Orders;
5.1.1. to receive information about Accounts and transactions;
5.1.2. to submit applications and conclude agreements with the Bank about use of various Services or termination of further use of Services.
5.2. PNB Internetbanka can be accessed at https://www.ib.pnbbanka.eu.
5.3. To be able to use PNB Internetbanka the Client needs Internet Explorer (version 9.0 or more recent) and a compatible web navigation system that supports JavaScript, as well as a connection to the Internet.
5.4. PNB Internetbanka can be accessed round-the-clock.
5.5. If the Client chooses to use the Mobile Application, he/she may use the Service to the extent ensured by the Mobile Application.
5.6. Use of the Mobile Application is subject to the conditions for use of PNB Internetbanka.

6. Use of PNB Vision

6.1. PNB Vision enables the Client with the help of a modem or by means of other Internet connection:
6.1.1. to manage money in Accounts submitting electronic Payment Orders to the Bank;
6.1.2. to receive information about Accounts and cash flow;
6.1.3. to submit applications and conclude agreements with the Bank about use of various Services.
6.2. The Client needs a computer with MS Windows 98/NT/2000/XP operating system, a modem or other connection to the Internet to use PNB Vision.
6.3. The Client's Electronic Identification Data for PNB Vision is: PNB Vision Password and/or the Electronic Signature.
6.4. PNB Vision can be accessed round-the-clock.

7. Use of PNB Trade (as a part of PNB Internetbanka)

7.1. If the Client uses PNB Internetbanka, he/she may also use PNB Trade, which enables him to conclude currency purchase and sale transactions with the Bank.

7.2. To start using PNB Trade the Client must apply to the Bank for the currency purchase and sale Service, and, if necessary, to conclude an agreement with the Bank on purchase and sale of non-cash currency in marginal accounts. Currency purchase and sale transactions and non-cash currency purchase and sale transactions in marginal accounts are concluded in compliance with regulations for concluding such transactions.

7.3. PNB Trade can be accessed round-the-clock.

8. Use of PNB SMS-Banka

8.1. PNB SMS-Banka enables the Client to receive information about the balance of the Account and any changes of the Accounts balance.

8.2. The Client requires a mobile phone with the function of dispatch and receipt of short messages (SMS) and/or e-mail to be able to use PNB SMS-Banka.

8.3. The Client's Electronic Identification Data for use of PNB SMS-Banka is the Client's mobile phone number, which he/she has indicated to the Bank, and the Electronic Signature.

8.4. The Client must ensure that third parties have no access to his mobile phone, e-mail and information sent to them from the Bank, as well as information and instructions sent to the Bank from them.

8.5. The Client must safeguard and prevent access of any third parties to the mobile phone number registered for use with PNB SMS-Banka (including prevention of its registration to the name of a third party). The Client must notify the Bank immediately, if he/she loses ownership of the mentioned number or switches to another mobile operator, or changes his/her number.

8.6. If the mobile phone number registered with PNB SMS-Banka is outside the reception area or is switched off for more than 3 (three) Banking days, the Bank does not ensure provision of the service to the Client and:

8.6.1. the Bank has the right to refuse to complete Payment Orders submitted by the Client and/or terminate the respective Remote Service;

8.6.2. the Bank bears no responsibility for losses incurred by the Client as a result of third party access and/or use of PNB SMS-Banka.

8.7. The Bank bears no responsibility in case any third parties gain access to information sent to the Client's mobile phone or e-mail, or information or Payment Orders sent from the Client's mobile phone.

8.8. Access to PNB SMS-Banka is ensured round-the-clock.

8.9. If the Client's settings for receiving information about transactions performed using the Card are different, information will be sent with PNB SMS-Banka's name number "PNBBanka".

9. Use of infoLINE

9.1. infoLINE enables the Client to receive information about Accounts by telephone.

9.2. The Client needs a telephone connected to a telephone network to receive information.

9.3. The Client must visit the Bank or contact the Bank's specialist on the round-the-clock telephone +(371) 67041118 and provide information requested by the Bank's employee, if he/she wishes to start using infoLINE. After completing the connection of the service and receiving the required information the Bank's employee gives the Access Code to the Client. The Access Code will be necessary to use infoLINE in the future.

9.4. Information through infoLINE is available round-the-clock. Telephone numbers for receiving information: +(371) 67011566 (information in Latvian) and +(371) 67011565 (information in Russian).

9.5. The following are the Electronic Identification Data of the Client for infoLINE:

9.5.1. to receive information about the Account – the Client's Code (CIF) assigned to the Client by the Bank at the time of opening the Account and the Access Code assigned by the Bank, when connecting the Client to infoLINE;

9.5.2. to receive information about the Card Account – the last 6 (six) digits of the Card Number and the Access Code the Bank issued to the Client, when connecting him/her to infoLINE;

9.6. The Client is identified with infoLINE based on the Electronic Identification Data indicated in Clause 9.5 of these Provisions using the phone's keyboard.

10. Use of PNB Chat

10.1. PNB Chat enables the Client to contact the Bank on-line to learn the possible terms of non-cash currency purchase and sale transactions, and to conclude such transactions with the Bank. Currency purchase and sale transactions are concluded according to Provisions of the respective Service.

10.2. The Client must submit an application through PNB Internetbanka to start using PNB Chat. After receiving an application from the Client the Bank registers the Client in PNB Chat and through PNB Internetbanka sends him/her the Electronic Identification Data of the Client (including PNB Chat Password) to access PNB Chat.

10.3. The address for accessing PNB Chat: https://chat.pnbbanka.eu.

10.4. To be able to use PNB Chat the Client requires Google Chrome or Mozilla Firefox browser supporting JavaScript and a connection to the Internet.

10.5. PNB Chat can be accessed round-the-clock, however, the Client may contact the Bank on-line and conclude transactions on days, when Latvian and foreign banks are open for financial operations with the respective currencies during these hours (Latvia time): for the residents of the Republic of Latvia from 8.00AM to 6.00PM and non-residents of the Republic of Latvia from 8.00AM to 6.30PM.

* * *