

Part F

REGULATIONS ON REMOTE ACCOUNT MANAGEMENT SERVICES

Terms used in the Regulations:

User – the Customer or other legal entity that has been designated and authorized by the Customer to use Remote Account Management Services to the specified amount.

Remote Account Management Services – Privat24^{EU}, Privat B@nkNet, Telephone Bank.

Remote Account Management Systems – Privat24^{EU}, Privat B@nkNet.

Authorisation Tools – special technical devices or parameters, which the User uses for attesting of the Transaction Document and Notification and their sending for execution to the Bank, and which provide the identification of the Customer/User and the authenticity of the Transaction Document and Notification. The Authorisation Tools are as follows:

Signature Password – a combination of digits and/ or letters of the Latin alphabet issued to the User by the Bank or created by the User.

Electronic Signature – a combination of digits and/ or letters of the Latin alphabet generated by the User.

Code Card – a plastic card with the digital Authorisation codes, issued by the Bank.

Digipass Device – an electronic device issued by the Bank and generating digital signature codes.

The Digipass Device is an independent remote account management tool for execution of Transactions; it can also be used for approving the Transaction Document and Notification by fax or e-mail.

Telephone Bank – remote account management for execution of Transactions between the Bank and the User via telephone communication with the Bank. The Bank provides Customer information and services pursuant to Paragraph 14.9. of the Regulations or receives information from Customer via telephone according to the Part B Regulations on Providing and Receiving Information and Services via Telephone and Online Chat. The Telephone Bank is available calling at the telephone number specified by the Bank for rendering the Telephone Bank services during Bank's working days and during its defined working hours. The Code Card and/or the Digipass Device can be employed as Telephone Bank's authorisation tools.

Bank provides password according to Customer's choice for Telephone Bank's usage:

Password - a Customer's Identification Code, which is chosen by the Customer and consists of Arabic numerals and/ or letters of the Latin alphabet, applied for at the Bank. The Customer is entitled to apply for the Password by completing, signing and submitting to the Bank an application in writing for opening of Account or an application for assigning of Password. The Customer may apply for the Password by completing, signing and sending an application for assigning of Password to the Bank by means of the Remote Account Management System.

Privat24^{EU} (Privat Online) – a Remote Account Management System for execution of Transactions and exchange of information between the Bank and the User in "online" regime by using the protected data transmission channels in the Internet. Privat24^{EU} is available in online mode on the web page address <https://ibank.privatbank.lv/> or using the Bank's Internet homepage www.privatbank.lv.

To manage the user accounts in the Privat24^{EU} system, the User needs to have the access to any computer connected to the Internet and use the browser. The Authorisation Tools in the Privat24^{EU} system may be the Signature Password, Digipass Device, Code Card.

Privat B@nkNet – the "client-bank" Remote Account Management System for execution of Transactions and exchange of information between the Bank and the User in the Internet by using the protected data transmission channels.

To be able to operate Privat B@nkNet the User needs to install Privat B@nkNet software suit available on the Bank's Internet homepage to a personal computer with the Internet

connection. The Authorisation Tools for Privat [B@nkNet](#) may be the Electronic Signature, the Digipass Device.

The Bank issues the following access parameters for the use of the Privat24^{EU} and Privat [B@nkNet](#) system:

- **User Name** (log-in name) – a combination, created from the letters of the Latin alphabet, which is meant for the User's identification in the Remote Account Management System.
- **Access Password/ Connection Password (access password to the program)** – a combination, created from the letter of the Latin alphabet and/or Arabic digits, which provides the possibility to use it and determines the User's access level to the Remote Account Management System.

18.1. Present Regulations on Remote Account Management Services are applicable, if the Customer/User has applied or already uses the Remote Account Management Systems, Telephone Bank and/or Authorisation Tools.

18.2. The User/Customer agrees that the Bank is entitled unilaterally at any time to determine the limitations for conclusion to the remote management of accounts and execution of Transactions by means of the Telephone Bank and/or Remote Account Management System, and the User/Customer undertakes to observe them without reservation.

Application for Use of Remote Account Management Services

18.3. The Customer submits the application for the use of Remote Account Management Services to the Bank, specifying the relevant Remote Account Management Services, Authorisation Tools and access modes in accordance with the limitations determined by the Bank.

18.4. The Remote Account Management System Privat24^{EU} is available in the following modes:

18.4.1. the informative mode – with the right to see the balance of accounts and receive other information about the accounts but without the right to prepare and send documents to the Bank;

18.4.2. the limited mode– with the right to prepare documents, but without the rights to send them to the Bank, and to receive all information about the accounts;

18.4.3. full access mode – with the rights to prepare documents and send them to the Bank, execute Transaction defined by the Bank, receive all information about the accounts, as well as receive other offers provided by the Bank and use Remote Account Management systems.

18.5. The Telephone Bank is available with the right to give orders regarding execution of payments, funds transfers, execution of Transactions and operations with the funds available on the accounts, conclude Transactions (authorize Transaction Documents and Notifications, sign agreements), as well as execution of other operations determined by the Bank.

18.6. The Bank upon receiving the Customer's application for the usage of the Remote Account Management Services and its verification prepares and issues unique parameters for access to the Remote Account Management System and/or the Authorisation Tools to the User. The Customer's account is connected to the Remote Account Management Services (systems)/Authorisation Tools/Access parameters after the Bank has received and verified the signed Customer's/User's Acceptance Protocol of Remote Account Management System access parameters and/or Authorisation Tools, if the Customer has an open (and activated) account at the Bank.

18.7. If the Customer – private individual has already been using the Remote Account Management Systems, then in case of opening new accounts at the Bank, these accounts depending on their type are connected to the existing Remote Account Management System.

18.8. If the Client – legal entity has already been using the Remote Account Management Systems, then in case of opening new accounts at the Bank, the Customer has to submit to the Bank application of a certain type:

18.8.1. on issue of new Remote Account Management System's access parameters/Authorisation Tools for the new accounts opened by the Customer;

18.8.2. on connection of the new accounts opened by the Customer to the existing Remote Account Management System.

18.9. The Customer/User is obliged to personally familiarise himself with the Regulations, the Installation of Remote Account Management Systems manual and Authorisation Tools application regulations (User manual, User guide). The documents, mentioned in the present Paragraph are available for the Customer/User at the Bank or on the Bank's Internet homepage – www.privatbank.lv.

18.10. The Bank issues access parameters for the Remote Account Management system to the User sealed.

18.11. The Password, the access parameters and/or the Authorisation Tools are confidential information, which the User and the Bank undertake not to divulge to third parties, as well as undertake to take all measures to prevent the possibility of divulging it to third parties. The User is obliged to safe-keep the confidential information, as well as to change the Password at any time, as well as in due term to change the Access Password and Signature Password.

User Identification. Security.

18.12. The Password and other data, which the Bank demands from the Customer (name, surname, personal identity number, passport data, company name, registration number, Account number and other), are the Customer's identification tools in the course of usage of the Telephone Bank by the Customer. The Bank is entitled to demand from the User and for identification purposes code from the Code Card or the code generated by the Digipass device.

18.13. When the User is connecting and operating in the Remote Account Management Systems, the Bank automatically identifies the User according to the User Password and Access Password.

18.14. In case the Authorisation Tool is lost or stolen, or the Password/codes from the Code Card/PIN-code from the Digipass device/User name, Connection Password/Access Password and/or Signature Password has become known or could have become known to a third party due to the reasons, irrespective of the User and/ or against the User's will, the Customer/User is obliged immediately to report it to the Bank orally or in written. The Bank blocks the access to the corresponding Remote Account Management Services within 1 (one) Bank Working Day of receiving the notification.

18.15. In case the User gives oral instruction to the Bank to block the access to the Remote Account Management Services, then the Bank performs the User's identification according to the User name/Password and other information at the Bank's disposal. Within 3 (three) Bank Working Days of receiving an oral instruction the Customer is obliged to submit a written Notification to the Bank in relation to the blockage of the corresponding Remote Account Management Services.

18.16. Taking into account the Customer's wishes the Bank provides, produces and issues to the User new unique access parameters for the Remote Account Management System and/ or issues new Authorisation Tools according to the procedure specified in the paragraphs 18.6.-18.8. of these Regulations.

18.17. If the Bank has reasonable suspicions, that the User has lost control over the confidential information, issued by the Bank by means of which the User may use the Remote Account Management Services (User name, Connection Password/Access Password and/or Authorisation Tools), as well as if the features of forgery of signature and/ or seal are stated in the Acceptance Protocol of Remote Account Management Authorisation Tools, the Bank is entitled, but not

obliged, to block the User's access rights to the Remote Account Management Services bearing no responsibility for it.

18.18. The User's access rights to the Remote Account Management System are automatically blocked, if during the connection to the Remote Account Management System the Access Password is input incorrectly 5 (five) times in succession or the Connection Password is input incorrectly 3 (three) times in succession.

18.19. The Authorisation Tool is automatically blocked and access rights to the Remote Account Management Services accordingly in case:

- the Signature Password is input incorrectly 3 (three) times in succession;
- the code from the Code Card is input incorrectly or called incorrectly 3 (three) times in succession;
- the code generated by the Digipass Device is input incorrectly or called incorrectly 3 (three) times in succession.

18.20. The Digipass Device is irreversibly blocked, in case:

- the 5-digit PIN-CODE is input incorrectly 3 (three) times in succession (for Digipass device models 500/550/280) ;
- the User attempts to open the Digipass Device or causes other mechanical damages to it (pours it with liquid, breaks it, and other).

18.21. User access rights (parameters) to the remote account management system/services and means of authorization if they are automatically blocked pursuant to Paragraphs 18.18. and 18.19. can be unblocked after presenting a written Notification by the Bank's Customer/User on their unblocking or orally via phone notifying the Bank on that pursuant to Part B of the Regulation on Submitting and Receiving Information via Telephone and Online Chat.

18.22. If the error is detected in the software of the Digipass Device the Bank shall replace the Digipass Device for the User for free.

18.23. In case of the irreversible blockage of the Digipass Device due to the reasons, provided for in Paragraph 18.20. the Bank shall perform the replacement of the Digipass Device, charging the Fee in accordance with the Bank's Fees.

Confirmation and Sending of Transaction Documents and Notifications to the Bank

18.24. The Customer and the User agrees that The Transaction Documents and Notifications, in case they are confirmed with the Signature Password/Electronic Signature/code from the Code Card and/or code generated by the Digipass Device in Remote Account Management Services procedure, specified by the Bank, are true and binding upon Customer, User and Bank, and are considered to be documents of equal strength, compiled and signed in written (paper) form in the understanding of the Civil Code of the Republic of Latvia with full legal force and legal effects and legal consequences, arising from it. The Customer cannot contest the Transaction Documents and Notifications, which have been submitted to the Bank by means of the Remote Account Management Services.

18.25. The code from the Code Card and/or code generated by the Digipass device serves for identification of the User. The Signature Password, Electronic Signature, code from the Code Card and/or code generated by the Digipass device serve for verification of authenticity of Transaction Document and Notification. Authorisation of Transaction Documents and Notifications with Signature Password, Electronic Signature, code from the Code Card and/or code generated by Digipass device is considered to be the Customer's own signature, that imposes liabilities onto the User in compliance with the norms of signatures and authorisation of the Civil Code of the Republic of Latvia.

18.26. The Transaction Document or Notification, compiled in accordance with the regulations of the Remote Account Management Services application manual (User manual/ User guide) and signed with Signature Password, Electronic Signature, code from the Code Card and/or code

generated by Digipass device is considered the User's instruction to perform Transactions and provide financial services.

18.27. The Bank is entitled not to execute the User's Notification (Transaction Document) compiled as the Transaction Document, if:

18.27.1. the User does not observe the present Regulations and the User guide instructions of Telephone Bank, Privat24^{EU}, Privat B@nkNet;

18.27.2. the User during the use of the Telephone Bank has not approved the content of the Notification (Transaction Document);

18.27.3. the Bank has suspicions about the User's identity and the Bank failed to contact the User to verify his identity and content of the (Notification) Transaction Document;

18.27.4. there is an insufficient amount of funds on the account for execution of Notification (Transaction Document) and payment of the fee charged by the Bank;

18.27.5. the Transaction limit defined by the Bank is exceeded;

18.27.6. the User's Notification (Transaction Document) is corrupted or not clear due to transmission interruptions;

18.27.7. the User does not observe other requirements of the Bank.

18.28. Upon the receipt of Transaction Document or Notification the Bank is entitled to contact the User repeatedly and verify if the Transaction Document or Notification is correct.

18.29. The Customer agrees that the Bank has the right with the help of the technical means to record the information (including telephone conversations) that has been conveyed during the use of the Telephone Bank. The Bank and the Client agree that such records of the Bank are considered as sufficient evidence of the communication via telephone between the Bank and the Customer and can be used as evidence in court.

18.30. The User's Notifications (Transaction Documents) on execution of payments and transfers shall be executed only within the limits determined by the Bank.

Liability

18.31. The Bank is not financially responsible for losses, which have arisen / may arise for the Customer due to communication line damage or interference or in cases when the Remote Account Management Services or their separate functions are unusable/ unavailable for the User due to technical reasons for execution of Transactions and operations and/ or the Transaction Document/Statement is not received in the Bank.

18.32. The Bank bears no responsibility for the Customer's losses, which may arise in connection with User's registration, cancellation or changes in the User's rights in case the Bank acts according to the User's Notifications, including the case when violations of procedure of the User's decision-making are stated.

18.33. The Bank is not financially responsible for any losses, arising for the Customer or may arise when submitting a Notification to the Bank by means of the Remote Account Management Services.

18.34. The Customer/User is responsible for his own actions and undertakes to indemnify all the losses to the Bank, which have arisen as a result of his actions.

18.35. The User bears responsibility for the User taking all the managerial security measures to prevent the access of unauthorised persons to the Remote Account Management Services, safekeeping and using of Password, User name, Access Password/ Connection Password and Authorisation Tools in the way to prevent the possibilities of its use by unauthorised persons.

18.36. The Bank bears no responsibility for the Customer's losses in case unauthorised persons connect to the Remote Account Management Systems and/ or use the Remote Account Management Services (access parameters/Authorisation Tools), as well send to the Bank the Transaction Documents or Notifications signed with the Signature Password, Electronic Password, code from the Code Card and/or code generated by the Digipass device, and the Customer/User has not reported it to the Bank.

18.37. The Bank bears no responsibility for execution of Transactions or operations, including the write-off of funds from the Customer's accounts in compliance with forged documents or otherwise unlawfully compiled/ submitted Documents, if these documents have been confirmed by the Signature Password, Electronic Password, code from the Code Card and/or code generated by the Digipass device.

18.38. The Customer undertakes all the risk and responsibility for losses which arise:

18.38.1. In case of erroneous or corrupted transmission of the Transaction Document or Notification, including miscomprehension, lack of infrastructure of technical communications or the errors, caused by disturbance, or corruption, so far it has not occurred due to the Bank's gross inattention;

18.38.2. in case of unlawful actions by third parties until the Remote Account Management Services are blocked according to the procedure defined in the Paragraphs 18.14. and 18.15.;

18.38.3. in case of duplication of the Transaction Document or Notification;

18.38.4. if the User has voluntarily passed the access parameters/Authorisation Tools to a third party's use and this third party has used the Remote Account Management Services;

18.38.5. if the User has not observed the present Regulations.

18.39. The Bank is entitled on its own initiative at any time to terminate the providing of Remote Account Management Services, informing the Customer/User about it.

Copyrights, Modifications

18.40. All the private and property copyrights for the Remote Account Management Systems software and related materials provided to the User (User manual, User guide, Remote Account Management Systems installation manual and other) are the property of the Bank. The User is entitled to use the systems software solely within the framework, specified in the present Regulations, i.e. in compliance with the regulations, specified in the application guide of the Remote Account Management System, determined by the Bank.

18.41. Without the Bank's consent any transformation of the Remote Account Management System software, any reproduction, publishing, any transfer to third parties and the use of technologies of the Remote Account Management Systems software in order to create other software, not stipulated in the present Regulations, which would execute the functions of the Remote Account Management Systems, is prohibited.

18.42. In case the Bank submits a new Remote Account Management System software version to the User the Bank is entitled to suspend the use of the previous software version.

18.43. The Bank guarantees the compatibility of Remote Account Management System software with the computer programs, indicated by the Bank.

Fees

18.44. The User shall pay the Fee to the Bank in accordance with the Bank's Fees for the use of the Remote Account Management Services, the issuance of its access parameters/Authorisation Tools, replacement, as well as in other cases, specified in the Bank's Fees.

18.45. The Bank on a no contestation basis writes off the relevant Fees from the Customer's accounts with the Bank or the User pays them in cash.