

netBanking

Terms and Conditions

1. Introduction

These Terms and Conditions of Sparkasse Bank dd govern rights, obligations and conditions pertaining to the use of the netBanking service, accessible through the global electronic network, the Internet.

NetBanking service is aimed at domestic and foreign legal entities that have transaction account with the Sparkasse Bank dd.

Meaning of words and expressions in these Terms and Conditions:

- Account owner – legal entity that has transaction account with the Bank;
- Contact person – official appointed by the legal representative of the business entity in charge of taking over the identification devices for all users;
- User – person authorized by the legal representative to use netBanking services; may be either signatory or officer;
- Signatory – person authorized by the legal representative to dispose of the funds on the accounts and sign electronic payment orders;
- Officer – person authorized by the legal representative to prepare electronic payment orders and co-sign them;
Note: although officers may co-sign orders, they are not considered eligible until signed by a signatory;
- Token generator – identification device that enables you safe access to netBanking;
- PIN – personal identification number – code disabling unauthorized use of token generators;
- Payment order – electronic order to the Bank with the successfully identified member ordering completion of a banking service. Such order has the same value as hand signed payment order.
- FAT member – enabled offline work and transfer of orders to other programs;
- THIN member – enabled only online work and disabled transfer of orders;

2. Approval of access to netBanking

To be allowed access to the service, account owner shall fill out and sign the Application Form.

The Bank shall check the data on the account owner and, if there are no overdue payables to the Bank, approve use of the service latest within 3 days.

Legal representative of the business entity may authorize one or more persons to use the netBanking services. Each user shall be issued identification devices, which shall be taken over and distributed to the users by the authorized contact person.

3. Payment order completion conditions

Once a payment order enters the Bank's information system, and the Bank confirms its reception by issuing a unique transaction number, such order is considered taken over, and the Bank assumes responsibility for its execution.

Payment orders shall be executed in due time and in line with the Bank's business policy and practice, as well as in line with the current exchange rate of the Bank.

Payment orders to be executed across the border do not have to be accompanied by invoices or other related documents by suppliers or service providers to whose accounts payment is done, but such documentation shall be kept in the files of the business entity, as defined by the Law.

In case a payment order is not eligible for execution, it shall be awarded status "rejected" and filed away.

4. User's obligations

The service user shall keep token generator, password and PIN code in a safe place and shall not share them with another person. If the service user suspects or finds out that their password was used by another person, the service user has the obligation to change such password (as described in the NetBanking Instructions). For any additional information, service members can contact user support unit at: 033 280 292 or netbanking@sparkasse.ba, from 8.00 AM to 5.00 PM.

Service user shall adhere to these Terms and Conditions and NetBanking Instructions.

Token generators are property of the Bank, and in case it is lost or service is canceled, service members shall return token generators or repay the value of a replacement token generator as defined in the Tariff.

5. Business entity's obligations

The business entity shall issue payment orders not exceeding the amount available on the transaction account with the Sparkasse Bank p.l.c. and meet minimum technical conditions defined in the item 12 of these Terms and Conditions.

The business entity shall appoint contact persons who will be in charge of taking over security devices and distributing them to the users.

Legal representative of the business entity shall inform the Bank on any change in the user status (signatory-officer) or cancellation of authorizations given to the user. The Bank shall act upon such information on changed or cancelled status immediately after such information is received via fax or registered mail sent to the office where netBanking Application Form was submitted.

If such information was sent to the Bank via fax, legal

representative shall main the original copy of the request to the Bank latest within the following day. Upon reception of such information, the Bank shall change/terminate the netBanking service user status. If user status is terminated, business entity shall return the users identification devices to the Bank.

The business entity (legal representative, contact person or user) shall report loss or theft of identification devices to the Bank during office hours, 8.00 AM to 5.00 PM at: 033 280 292.

The Bank shall not be held liable for the damage that occurred before the loss or theft was reported. The Bank shall charge all costs of the issuance of a new token generator according to the current Fee Tariff and its possible amendments.

Business entity shall be held liable for the damage that occurs as a result of inappropriate handling of identification devices (PIN code and token generator).

6. Bank's obligations

The Bank executes payment orders in line with the Terms and Conditions and with other relevant contracts and terms and conditions signed with the business entity in line with relevant laws. All actions of users shall be recorded electronically. Electronic records of such actions are filed with the Bank.

If the business entity has provided users' email addresses to the Bank, the Bank will inform the users on all relevant news.

The Bank shall not be held liable for any disturbances and disruptions in the telecommunication network and access to netBanking system, or damage caused therein, regardless of the cause.

7. Service fees

Fees for netBanking services and additional token generators shall be charged by the Bank in line with the current Fee Tariffs one time.

8. Claims and complaints

The business entity may file a complaint on execution of payment orders or information on incoming funds sent via netBanking to the Bank as defined in the Terms and Conditions.

9. Blocking netBanking services

The Bank shall block access to netBanking to users for which user status was terminated by legal representative of the business entity. If a user finds that their identification devices were misused by another person, they shall inform the Bank as soon as possible. Upon reception of such information, the Bank shall block access to netBanking for such user. If the bank suspects or discovers that there is a possibility of manipulation of netBanking services, access to the service shall be blocked

and business subject duly informed. The Bank shall also block access to the service in case minimum conditions defined in the item 12 herein have not been met.

10. Cancelation of netBanking services

NetBanking services may be cancelled upon written request of the business entity. Upon such cancelation, the business entity shall return identification devices to the Bank.

The Bank shall cancel netBanking services in case that business entity's actions breach Terms and Conditions agreed with the Bank.

Business entities whose netBanking services were canceled by the Bank shall return identification devices and all other equipment necessary for the access to the service to the Bank, and cannot apply for netBankin services again.

11. Personal data

Users hereby authorize the Bank to keep their personal data in its database. The Bank shall use personal data solely for the purposes of rendering netBanking services and dissemination of information on its services.

The Bank shall disable unauthorized access to users' personal data and shall not use any of the data in purposes other than the ones described in paragraph 1 herein.

Data on operations through netBanking system are considered confidential and can be revealed to third persons only if so defined by the law.

12. Minimum technical conditions for netBanking services

Business entities shall meet minimum technical conditions needed for this services, as follows:

- PC with adequate configuration,
- rented or dial-up internet connection;
- internet browser, i.e. Internet Explorer 6.0 or higher, with support for 128 bit encryption;
- Mozilla Firefox 3.0 or higher with support for 128 bit encryption of operations between the server and client accounts
- Adobe Acrobat Reader 4.0. or higher,
- Flash Player 10.

13. Final provisions

These Terms and Conditions are a part of the Application form and by signing the application form the business entity confirm their acceptance on the date of submitting the application.

If the business entity disagrees with the Terms and Conditions, it may cancel the service as defined in the paragraph 10 herein.