SBERBANK

Business terms for online banking

Effective from 17/ 4/ 2020

BUSINESS TERMS FOR ONLINE BANKING BANKING – SBERBANK ONLINE BANKING

Part I Introductory provisions

(1) These Business terms for online banking (hereinafter the "**Terms and Conditions**") set out binding rules for electronic communication with the bank – Sberbank Online Banking, Sberbank Online, Smart Banking and Sberbank Online Mobile between Sberbank CZ, a.s., Reg. No.: 25083325, registered in the Commercial Register at the Municipal Court in Prague under File Ref. B 4353 (hereinafter the "**Bank**"), and the Bank's client (hereinafter the "**Client**") and the user of the online banking (hereinafter the "**User**").

Part II Definition of Terms and Product Description

(1) **Online banking** is an electronic banking service that enables the Client and the User to electronically access and manage the Client's account(s) (hereinafter the "Account") maintained by the Bank, and displays any other products that the Client has arranged with the Bank.

(2) **Sberbank Online Banking, Sberbank Online, Sberbank Online Mobile and Smart Banking** are applications through which the Bank provides online banking to its Clients.

(3) **The Client** means a person who concluded a Contract with the Bank, i.e., the Account holder.

(4) **The User** means a person authorised in the Contract by the Client to electronically access the Client's Accounts within his/her online banking.

(5) **The Administrator** means a person authorized in the Contract by the Client to administer the signature rules within the online banking.

(6) **User authentication** is the identity verification of the User when logging into the online banking. It is provided by so-called security elements according to the access manual for a specific application pursuant to (2) of this section of the Terms and Conditions.

(7) **Authorisation** means confirmation of the operations. Authorisations of active and passive operations are specified in the application-specific user manuals listed under (2) of this section of the Terms and Conditions.

(8) **Active user** means a user authorised in the Contract to monitor the Client's Account balance and to perform active operations.

(9) **Passive user** means a user authorised in the Contract to monitor the status of the Client's Account and to perform the operations specified below in Clause (13) of this section of the Terms and Conditions.

(10) The Client's primary duty is to comply with the Contract and these Terms and Conditions and to ensure that Users comply with their obligations set out in the Contract and the Terms and Conditions. The Client acknowledges that the Bank's instructions and recommendations regarding the use of the Online Banking System can be found on the Bank's website at www.sberbank.cz in the Sberbank Online Banking and Sberbank Online applications, and in the User Manual section.

(11) The User's authorisation to access the Client's Accounts via online banking shall expire at the latest on the Bank Business Day following delivery of a written withdrawal of the power of attorney for the User by the Client or a written termination of power of attorney by the User to the Bank.

(12) **Applications:**

a) Sberbank Online Mobile is an application that the Client installs on his/her mobile device with an Android or iOS operating system, most commonly a mobile phone or tablet), hereinafter the "**Mobile device**") and serves for electronic communication with the Bank;

b) Sberbank Online is a web application which is accessible at www.sberbank.cz and serves for electronic communication with the Bank;

c) The Mobile token is an application that the Client installs on his/her Mobile device and is used for Authentication and Authorisation (hereinafter the "mToken").

d) Smart Banking is a banking application that allows the Client/an active user, through a Mobile device of such Client/User, to dispose of funds in Accounts maintained by the Bank and perform other acts/operations. Smart Banking serves for electronic communication with the Bank.

Detailed information about each application is available in the user manuals.

(13) **Online Banking Security Features:**

a) **Log-in name**

Unique piece of information generated by the Bank for the Client or chosen by the Client at the Bank's Point of Sale or electronically. The Client may change the Log-in name.

b) **SMS code**

A unique code that serves for Authentication and Authorisation of operations. It is sent to a unique Security phone number.

c) **Security phone number**

A phone number which is specified in the Contract, and which the Client has registered at the Bank. The Client may change the Security phone number at the Bank's Point of Sale or through Sberbank Online, provided the Client has activated the mToken application. If the Security phone number for this purpose has already been registered at the Bank for another Client of the Bank, it is possible to assign this Security phone number to the Client at the Bank's Point of Sale and to remove it from another Client once the Security phone number has been verified by a Bank employee.

d) **mToken**

A mobile app that serves for Authentication and Authorisation of operations. It can be activated and deactivated via Sberbank Online. To use the MToken application, you need a Mobile device and the mToken application, which is available from the official App Store and Google Play. Use of the mToken application is bound to one specific Mobile device. The Client performs the registration in Sberbank Online, uses the QR code from Sberbank Online and the SMS code. He/she chooses the mToken PIN upon registration.

e) **Password**

The Client chooses it upon registration in Sberbank Online. The password must comply with the minimum-security rules set by the Bank.

f) **Sberbank Online Mobile PIN**

The Client chooses it upon registration in Sberbank Online Mobile. The Sberbank Online Mobile PIN must

comply with the minimum-security rules set by the Bank.

g) **mToken PIN**

The Client chooses it when registering in the mToken application. The mToken PIN must comply with the minimum-security rules set by the Bank.

h) **Biometric element**

Serves for Authentication and Authorisation of operations. A biometric element means, for example, a fingerprint or face recognition and can only be used if supported by the Mobile device.

i) **Authorisation via Signature Certificate**

The security for working in Sberbank Online Banking is provided by the access data received by the User from the Bank and by passwords chosen by the User in the application. The access data are issued in security envelopes.

j) **Token authorisation**

Another type of security is a combination of access data ("Log-in name") and work with the token according to the Manual. The log-in name is assigned to the User in the form of a security envelope or the User chooses it when arranging the Online banking at a Point of Sale. The User can also receive a one-time log-in name via SMS. The User then selects a new log-in name when first logging in. The User will receive the token personally from the Bank and its issue will be subject to a fee according to the valid Schedule of Fees.

Part III Rights and Obligations of the Parties, Security

Article III.1 Rights and Obligations of the Parties, Security

(1) The Bank undertakes to provide the Client and the User with the relevant access information to enable the use of the online banking.

(2) The Client uses the applications used for online banking according to the applicable application manual.

(3) The technical equipment on which Sberbank Online Banking, Sberbank Online and Sberbank Online Mobile will be installed must comply with the technical requirements specified by the Bank as specified in the User Manual.

(4) The Bank shall activate electronic access to the Accounts within 3 (three) Banking business days from the date of conclusion of the Contract. Other deadlines for the processing of changes are specified in the Contract.

(5) In the case of using Sberbank Online Banking using the token, the Bank shall hand over the token to the User in person or by mail in a security envelope with the data necessary for access to the Sberbank Online Banking system. The User is obliged to only use the token for authentication in Sberbank Online Banking and for the authorisation of active operations according to the second part of paragraph (12) of the Terms and Conditions. The token is powered by a battery that is designed for the lifetime of the token. Neither the Client nor the User is authorised to attempt to replace or repair the battery. In case of problems with the token, the Client and the User contact the staff of the Bank and request a replacement token. The Client is responsible for any damage caused to the Bank by unauthorised handling of the token. The Client and the User shall return the token to the Bank upon the termination of the Contract.

(6) The Client / User is obliged to check the integrity of the security envelopes upon receipt. In the event of physical damage, the Client / User shall immediately notify the employee representing the Bank of this fact; if the security envelopes have been sent by mail, request confirmation of delivery of the damaged consignment from the post office and present this document to the Bank. Upon receipt of the notification as described in paragraph (10) of this section of the Terms and Conditions, the Bank is obliged to block access to the Online banking system and subsequently investigate whether any unauthorised use of funds or disclosure of data available in the application has occurred.

(7) All access data of the Online banking Users stated in the security envelopes are top secret. Users shall ensure that they are not disclosed to any third party. The Online banking User must not disclose his/her own PIN and passwords set in the Online banking to any third party or allow access to these PIN codes and other passwords to any third party; furthermore, he/she must not pass on the token, disclose the token code, or allow any third party to access the token code.

(8) The Bank shall not disclose the Users' access data to any person other than the relevant Online banking User.

(9) The Client and the User are obliged to comply with all agreed security procedures and measures when using the Online banking. The User Manual contains the section Ten Security Rules, in which the Bank sets out the basic security principles for using the Online banking. The Client confirms that he/she is familiar with these Rules.

(10) In case of loss/theft of the PIN, passwords, token or other access data, or if there is reasonable concern that a third party has acquired the access data that would allow them to misuse a Client's Account, or if there are other concerns about misuse of a Client's Account, the Contracting Parties shall inform each other without delay. The Client or the User of online banking on his/her behalf is obliged to notify the Bank of this fact without delay in one of the following ways:

a) by telephone to the online banking Infoline on 800 133 444, option 3, Mon–Thu 8 AM–6 PM, Fri 8 AM–4 PM

b) at any time electronically to the email address online-banking@sberbankcz.cz or

c) during the opening hours of the Call Centre to the Infoline on 800 133 444 (from abroad +420 543 525 901), or

d) in person at any Point of Sale of the Bank.

Immediately after making a report pursuant to the previous provisions of this paragraph, the Client is obliged to confirm the notification by submitting a written Request for blocking electronic access.

(11) The Bank may also block electronic access on its own initiative for reasons of security of electronic access, in particular, if it suspects its unauthorised or fraudulent use. The Bank shall inform the Client of the blocking and the reasons for it (however, this does not apply if the provision of such information could frustrate the purpose of the blocking or would be contrary to other legal regulations) before blocking electronic access or, if this is not possible,

immediately thereafter. Notification will be made by telephone. The Bank shall unblock electronic access as soon as the reasons for blocking cease to exist; the Client may request the unblocking in writing at any Point of Sale of the Bank.

(12) On the day of blocking electronic access to the Accounts, the Bank shall examine all outgoing payments, incoming payments, direct debits and standing orders not yet processed, and shall not make any unauthorised not yet processed outgoing payments, incoming payments, direct debits and standing orders. The Bank shall verify with the Client whether the outgoing payment, direct debits and standing orders were actually authorised. If the Bank fails to verify this fact with the Client, the Bank shall not make those outgoing payments, direct debits or standing orders until the Client allows the Bank to verify the outgoing payments, direct debits and standing orders.

(13) In the event of an emergency or for maintenance of the system, the Bank may, in urgent cases, suspend access to the Online banking or suspend the provision of some or all Online banking services without prior notice to the Client. The Bank shall immediately inform the Client of this fact.

(14) The Client bears the loss of any unauthorised outgoing payments, standing orders or direct debits up to a total amount of EUR 50 (fifty), if the loss was caused by the use of lost or stolen access data.

(15) The Client bears the loss of any unauthorised outgoing payments, standing orders or direct debits in its entirety if the loss was caused by his/her fraudulent conduct or by his/her intentional or gross negligent breach of any of the obligations laid down in Article 165 of Act No. 370/2017 Coll., on Payments, as amended.

(16) Except in cases of fraudulent conduct of the Client, the Client shall not bear the loss of any unauthorised outgoing payments, standing orders or direct debits if:

a) He/she could not have known of the loss, theft or misuse of the access data prior to the execution of the unauthorised outgoing payment, standing order or direct debit; or

b) The loss, theft or misuse of the access data was caused by the Bank 's conduct; or

c) The loss occurred after the Client had notified the Bank of the loss, theft, misuse or unauthorised use of the access data, or

d) The Bank did not ensure that he/she had the appropriate means at any time to report its loss, theft, misuse or unauthorised use, or

e) The Bank has breached the obligation to require strong verification in the cases required by legal regulations.

Part IV Terms & Conditions of Processing

(1) Any payment order submitted electronically using Online banking may be revoked until it is accepted in accordance with the Commercial Terms and Conditions of Payment. Upon agreement with the Bank, the Client may revoke a payment order (with the exception of consent to a direct debit) after its receipt by the Bank, but only on condition that the specific outgoing payment, direct debit or standing order has not been sent from the Bank or has not yet been executed , if it was a transfer within the Bank. The request for revocation of a payment order shall be submitted through an application in Online banking and can only be done by an Active Online Banking User.

Part V Settlement of Domestic and Foreign Payment Orders

Domestic Payment Orders

(1) In the case of domestic outgoing payments or standing orders which the Client and User requests to be processed as "**urgent**", he/she must check the Priority Payment option in the payment order.

Foreign Payment Orders

(1) In case of foreign payments which the Client and User requests to be processed as "**urgent**", he/she must check the "Urgent" option in the Payment Priority menu in the payment order.

(2) Payment orders for transfers between Accounts maintained by the Bank in different currencies and for transfers between Accounts maintained by the Bank in the same foreign currency, shall be submitted via the electronic form for Intrabank foreign currency payment orders.

(3) Currency conversion is performed by the Bank according to the exchange rate set and announced by the Bank in accordance with the Commercial Terms and Conditions of Payment at the time of execution of the order. The Bank is entitled to change the Exchange Rate Table up to the moment the payment order is processed, but such a change must be made in a neutral manner. Unless otherwise agreed, the Bank clears a foreign payment order or an intrabank foreign currency payment order using the "foreign exchange purchase / foreign exchange sale" rate valid at the time of processing the payment order. Exchange rates used by the Bank are accessible to the Client at all the Bank's Points of Sale, as well as on the Bank's website at www.sberbank.cz and in the Sberbank Online Banking and Sberbank Online applications.

Part VI Limits

(A) Limits for Online banking:

(1) The limits for Online banking are to be set by the Client in the specific application or at the Bank's Point of Sale. Increasing limits is allowed only at the Bank's Point of Sale. The maximum amount of the limits is stipulated by the Bank.

(2) The product limit for a specific account is set by the Client in the application as a daily or a monthly limit. It applies to the Client and the User together.

(3) The user limit for each User is set by the Client in the application as a daily limit. It applies to all Outgoing payments, Standing orders, Direct debits of the specific Users.

(4) The limits are stated in the domestic currency (CZK) if the Client has access to accounts in other currencies, Standing orders, Direct debits, Outgoing payments from these accounts are converted at the current exchange rate Foreign Exchange for the purpose of calculating the limit – the middle rate according to the Exchange rate list of the Bank. The limits apply to the Outgoing payments, Standing orders and Direct debits submitted during the day or month, depending on the setting of a specific limit, regardless of their due date.

(5) The limits do not apply to the Standing orders, Direct debits and Outgoing payments between own accounts.

(6) The limits are always restored from the beginning of a new day or month, depending on the settings of a particular type of limit.

(7) The signing rules are set in Online banking by the Client or the Administrator. They set the rules for Authorising the operations, set the limits and the number of persons who must authorise an operation before it is finally accepted for processing by the Bank.

B) Special limits for Sberbank Online Banking:

(1) An active User who uses a signed certificate for authorisation is entitled to hand over the payment orders for outgoing payment transactions to the Bank through Online banking up to the daily limit agreed in Online banking, at the Bank's Point of Sale or in the Contract. In the case of active Users with a signed certificate created prior to the effective date of these Terms and Conditions who do not have a limit agreed in the Contract, the above limit provision shall take effect from 1/ 4/ 2010, where from that date, these Users are only entitled to submit payment orders for outgoing payment transactions to the Bank up to CZK 20,000 (twenty thousand) per day.

(2) An active User who uses a token for authorisation is entitled to hand over the outgoing payments to the Bank via Sberbank Online Banking without limitation unless otherwise agreed in Online banking or in the Contract.

(3) The limit for the outgoing payments applies cumulatively to all Accounts made available to the User in Sberbank Online Banking and to the outgoing payments created in the period for which the limit is set. The limit does not apply to the outgoing payments submitted through Sberbank Online Banking between the Accounts maintained by the Bank within one User access to these Accounts and to the establishment of standing orders. User access is defined by the log-in name for Sberbank Online Banking.

C) Special limits for Smart Banking:

(1) In the case of using Smart Banking, the Bank sets the following limits for Users:

a) the transaction limit or the time limit agreed for the User within Sberbank Online Banking,

b) the Standard Authorisation Limit set by the Bank,

c) the limit for Subsequent Authorisation set by the Bank,

d) the global limit set by the Bank.

A global limit means the limit for the sum of the outgoing payments submitted to the Bank within one calendar day via Smart Banking. It includes all the outgoing payments submitted from a mobile device (regardless of the due date). If a time limit is agreed in the Contract, these outgoing payments shall be added to the outgoing payments sent to the Bank via Sberbank Online Banking in the specified time period. The Outgoing payments sent via Smart Banking thus reduce (i.e., use) the time limit in Sberbank Online Banking.

(2) A User is authorised to perform the outgoing payments via the Smart Banking application always up to the amount of the transaction and time limit, if agreed in the Sberbank Online Banking Contract, but not more than the global limit, which is determined by the Bank and amounts to CZK 20,000 (twenty thousand) per each calendar day. These limits apply cumulatively to all outgoing payments from all Accounts which are made available to the User in Smart Banking under the Contract on the Establishment of Smart Banking. The agreed limits do not include the established standing orders and term deposit accounts placed in Sberbank Online Banking, furthermore, they do not include the outgoing payments submitted through Smart Banking between the Accounts maintained by Sberbank CZ, a.s.

Part VII Prices of Services

(1) Unless otherwise agreed, the Client shall be charged for the provided services according to the valid Schedule of Fees from the account specified by the Client. However, the Bank is also entitled to charge a fee from any other account of the Client's.

(2) These fees include in particular: a one-time token issuance fee, a flat-rate fee for using Online banking and for reissuing the access data. The fee for the execution of a direct debit, standing order, outgoing payment and incoming payment, i.e., domestic payments, fee for execution of a foreign payment, intrabank payments, extra charge for an urgent payment, fee for revoking an outgoing payment and other surcharges related to the payment are primarily settled from the Account from which the payment was made.

(3) The Schedule of Fees is available at the premises of all the Bank's Points of Sale and on the Bank's website www.sberbank.cz. By concluding the Contract, the Client confirms that he/she has acquainted him/herself with its contents.

Part VIII Complaints

(1) The Client (or, on his/her behalf, an Active Online Banking User) is obliged to check in the Account Statement without undue delay whether the direct debits, standing orders, incoming payments and outgoing payments stated in it are authorised and correctly settled. If the Client detects discrepancies in the settling of direct debits, standing orders, incoming payments or outgoing payments, he/she is entitled to claim demonstrably any errors found with the Bank immediately after their identification, however, no later than 13 (thirteen) months after the funds are deducted from the Account. The Bank shall examine the rights raised by the Client and the Online Banking User within the set time limit. Further conditions are specified in the Bank's Complaints Procedure Rules, which are available on the premises of all the Bank's Points of Sale and are also published on the Bank's website www.sberbank.cz.

(2) If an incorrect direct debit, standing order, incoming payment or outgoing payment in accordance with these Terms and Conditions is claimed unsuccessfully and the Client is dissatisfied with such a solution, he/she has the right to contact a financial arbitrator who resolves any disputes between issuers and holders in issuing and using electronic means of payment pursuant to Act No. 229/2002 Coll., on the Financial Arbitrator, as amended, with its registered office at Legerova 1581/69, 110 00 Prague 1, www.finarbitr.cz. The right of the Client to address the court remains unaffected.

Part IX Amendments to the Contract/Terms

(1) The Bank is entitled to amend these Terms and Conditions in accordance with Part Three, Articles II / Conclusion and Changes to Contracts, and III / Changes to the Terms of the General Commercial Terms and Conditions.

Part X Transitional Provisions

(1) Issuing of the access data for the creation of the signature certificate is from 1/ 8/ 2015 no longer offered by the Bank.

Part XI Final provisions

(1) Should the provisions of the Terms and Conditions conflict with the provisions of the General Commercial Terms and Conditions, the Commercial Terms and Conditions for Payments or the Commercial Terms and Conditions for Current and Savings Accounts, the provisions of these Terms shall prevail.

(2) This Contract is governed by the laws of the Czech Republic.

(3) These Terms and Conditions shall take effect on 17/ 4/ 2020 and supersede the Business terms for Sberbank Online Banking of 15/ 11/ 2018.

Part XII Important provisions

(1) The Client is duly acquainted with the Contract, Terms and Conditions, User Manuals, Security Principles and Info sheets, accepts them and, in particular, expressly accepts the provisions in bold of the Terms and Conditions.

(2) These Terms and Conditions include the user manuals for Sberbank Online Banking, Sberbank Online, Sberbank Online Mobile, mToken, then the Security Principles and Info sheets for Sberbank Online Banking and Smart Banking. All documents are available on the Bank's website www.sberbank.cz in the Online banking section.