BUSINESS CONDITIONS OF PPF BANKA A.S. FOR INTERNET AND MOBILE BANKING

Contents:

1. Introductory provisions

1.1 These Business Conditions of PPF banka a.s. for Internet and Mobile banking (hereinafter the "**Specific Conditions**" or "**SBC**") lay down the rules governing the legal relationships arising during the provision and the use of the Internet Banking (hereinafter "**IB**") and Mobile Banking (hereinafter "**MB**") Banking Services.

1.2 The General Business Conditions of PPF banka a.s. (hereinafter referred to as the "**GBC**") and these SBC form an integral part of every Agreement. In the event of any conflict between the provisions of an Agreement, the GBC, the SBC, the Price List and the Interest Rate List, the following order of precedence shall apply: the Agreement, the SBC, the GBC, the Price List and the Interest Rate List.

1.3 These SBC have been issued under, and in accordance with, Section 1751 of the Civil Code and other applicable legal regulations.

1.4 These SBC are issued in accordance and conjunction with the GBC. Matters not provided for under the Agreement or the SBC shall be governed by the GBC.

2. Definition of terms and interpretation rules

2.1 The capitalised terms and expressions have the following meaning in the SBC:

Security Elements – in accordance with the GBC these consist primarily of the following: a Cronto code, a Token, an e-Token, an IB Login Password, an SMS code and an IB Username. For MB, they also include a PIN and Biometric Data.

Security Principles – the documents issued by the Bank that set out several recommendations concerning the secured use of the Services. The Bank will make available the current version thereof on its Website and in the Place of Business.

Biometric data – personal data for identifying natural persons, that can be obtained using a biometric reader and that is used as a Security Element for MB purposes. A fingerprint and a facial image are considered biometric data in particular.

Call centre – A provider operating the Hotline for Blocking Electronic Banking outside the operating hours of the Customer Service.

Cronto code – a special graphic cryptogram generated by the IB User and read using a Token or e-Token separately for:

- each login to the Services, to verify the IB User,
- Payment Orders or requests to the Bank, to authorise them.

This is not, however, an encrypted signature.

Batch – a file (generated e.g. by the Client's accounting system) in a format accepted by the Bank, whose content is a multiple Payment Order.

Debit Card – an electronic Payment Instrument issued for the Client's Payment Accounts in accordance with the rules of the relevant Card Association.

Supplier – a third party that processes or performs a service or services forming part of Services, or which contractually carries out activities for the Bank associated with the operation of Services.

e-Token – a mobile application for logging in to IB and for the authorisation of operations based on a Cronto code.

Main Client – the Bank's Client through whom a Client uses Services in part or in whole. The Client grants a power of attorney to the Main Client and his IB Users for the purposes and to the extent as may be necessary for the Client to use Services through the Main Client.

Internet Banking (IB) – an online system of ELB (operating via a continuous connection with the Bank) allowing an IB User to communicate with the Bank, to submit Payment Orders and requests to the Bank, and to obtain additional information, including information about the balance on Accounts and any Payment Transactions performed on them.

Limit – the maximum total amount that may be used in handling Funds in an Account, specified in the Authorisation. This Limit is always specified in CZK, and may be set for a Payment Order (hereinafter also referred to as the "Transaction Limit"), for a certain time period (Business Day, calendar week, calendar month or calendar quarter – hereinafter also referred to as the "Time-based Limit"), or in a combined form for a Payment Order and also for a certain time period. A Limit applies in aggregate to all the Accounts specified in the Authorisation, which may be handled by the IB User via Services.

Hotline for Blocking Electronic Banking – a telephone line for reporting the loss or theft of Security Elements for electronic banking or for reporting the misuse of electronic banking. The telephone number is available on the Website.

Mobile Banking (MB) – a mobile online application of ELB (operating via a continuous connection with the Bank) allowing an IB User to communicate with the Bank, to submit Payment Orders and requests to the Bank, and to obtain additional information, including information about the balance on Accounts and any Payment Transactions performed on them.

PIN – an authorisation four-digit identifier that an IB User can choose in order to login in MB (it is intended for IB User verification) and to authenticate Payment Orders or requests for the Bank. It is not an encrypted signature.

Authorisation – a form specified by the Bank, Authorisation of an Authorised Party for Payment Services, whereby the Client authorises an IB User to access Services. The Authorisation also sets out the range of the access rights and permissions, in particular, but without limitation, access to Accounts and to Payment and Banking Services, the right to submit Payment Orders and, if applicable, the right to authorise Payment Orders or to send requests to the Bank.

In relation to the Services that the Client uses through the Main Client and/or his IB Users, the Client's Authorisation is considered to be the Authorisation granted by the Main Client.

IB Login Password – assigned to each IB User. The IB User enters the IB Login Password when logging into IB and MB and when performing the registration of the Token or e-Token. An IB Login Password must have between eight to thirty characters, may contain only alphanumeric characters without diacritical marks, must include at least one uppercase letter, one lowercase letter and one digit, and may not contain any repetitions.

List of Accounts – a list of the Accounts which may be viewed or potentially handled via Services.

Service – an umbrella term for Internet Banking, Mobile Banking, the Account Information Service and the Payment Initiation Service, or any of the above Services referred to individually.

Account Information Service – means an online service to provide information on a Payment Account available in the Client's IB, which can be provided by the Bank or by the Third Party.

This service includes online confirmation of the balance of funds, consisting of the provision of information as to whether or not the balance of the Payment Account available in the Client's IB covers the amount of a card Payment Transaction being executed by the Provider issuing the card payment instrument who is requesting information on the balance, which can be provided by the Bank or the Third Party.

Payment Initiation Service – means an online service to initiate a Payment Order on behalf of the Client with respect to a Payment Account available in the Client's IB, which can be provided by the Bank or by the Third Party.

Agreement – an agreement concluded between the Client and the Bank under which the Client is allowed to use ELB, regardless of the name of such agreement.

SMS code – a unique, eight-digit numerical identifier for authorisation purposes which is sent to the IB User to a specified mobile telephone number. A unique SMS code is generated separately for:

- each login to Services, to enable IB User verification,
- Payment Orders or requests sent to the Bank, for the purpose of their authorisation.

This is not, however, an encrypted signature.

Technical Requirements – a set of requirements for software and hardware needed for ensuring the operation of Services on the part of the Client. The Bank shall publish the current wording of Technical Requirements on its Website.

Token – a hardware device used for logging in to IB and for the authorisation of operations based on a Cronto code.

Third Party – another Provider distinct from the Bank that is authorised to provide the Payment Initiation Service or the Account Information Service.

IB User – an Authorised Party authorised by a Client to use Services. The scope of an IB User's access rights and permissions is specified in the Authorisation. In relation to the Services that the Client uses through the Main Client, every Main Client IB User is regarded as a Client IB User.

IB Username – an IB User's login name for IB and MB agreed between a Client and the Bank and stated in the Bank-designated form ELB Access of an IB User. An IB Username must have between eight and sixteen

characters, may contain only alphanumeric characters without diacritical marks, must include at least one uppercase letter, one lowercase letter and one digit.

Multiple Authorisation – a system configuration where a selected number of authorisations from (2 or more) IB Users is required for the use of Services, regardless of the amount of any specified Limit.

Multilevel Authorisation – a system configuration where a selected number of authorisations from (1 or more) IB Users is required for the use of Services, depending on the amount of a specified Limit.

Customer Service – a telephone number or email address used for reporting faults or irregularities in Services and for providing user support to Clients and IB Users. Business Hours of Customer Service are available on Bank's Website.

2.2 Unless these SBC provide otherwise capitalized terms and expressions have the meaning given in the GBC.

2.3 The following rules shall be followed when interpreting the provisions of these SBC and the Agreement:

(i) Any reference to an article, paragraph, clause referenced by a letter, or point is regarded as a reference to an article, paragraph, clause referenced by a letter, or point of these SBC;

(ii) The headings of articles and paragraphs of the Agreement and these SBC serve for convenience only and not for interpretation;

(iii) Words and expressions in the singular also include those in the plural, and vice versa;

(iv) Agreement is understood to be an Agreement, including all of its integral parts, in particular, but without limitation, the GBC, the relevant SBC, the Interest Rate List and the Price List;

(v) The person representing the Client is understood to be the Authorized Person or any other person authorized to represent the Client;

(vi) **CZK, Kč** and **Czech crown** mean the lawful currency of the Czech Republic; **EUR** and **euro** designate the common currency of the European Union member states that will adopt or have adopted the euro.

3. General provisions

3.1 The Bank provides the IB Service under an Agreement, or upon the Client's request and its acceptance by the Bank.

3.2 The Bank makes it possible for Clients to use the Payment Initiation Service and the Account Information Service on the basis of explicit consent given by the Client.

3.3 Clients access Services through the Website. Clients may use Services only for the agreed purpose. The Client uses Services in person as an IB User or via IB Users.

3.4 The Account Information Service and the Payment Initiation Service can only be used in respect of Accounts accessible to an IB User via IB.

3.5 The Client acknowledges that, within the scope of their respective access rights and permissions, IB Users have access to information regarding the balance and the transactions performed on the Accounts which they work with in Services.

4. Technical requirements

4.1 The minimum technical requirements for the operation of Services are listed in the Technical Requirements.

4.2 The Bank may improve Services from time to time by upgrading them to a higher version; the Bank is obliged to inform Clients of any such planned upgrade sufficiently in advance of performing the upgrade.

4.3 Clients are obliged to ensure that they have HW which is adequate in terms of its functioning and performance and that any other installed SW is compatible with Services for the entire period of validity of the Agreement. In cases where Services are improved and/or upgraded to a higher version, Clients are obliged to ensure that their HW and SW meet the requirements for this change.

4.4 By signing the Agreement, or by submitting the documents specified by the Bank for the provision of a Service, the Client guarantees that it has adequate HW and SW for using Services to the extent of the Technical Requirements.

5. Services implementation

5.1 The Bank will provide IB to the Client only if the Client holds at least one Payment Account with the Bank.

5.2 The Bank will provide the Client with access to use IB on the basis of a concluded Agreement or on the basis of accepting the request for the provision of IB by the Bank, Authorisation of Authorised Parties, specification of the Accounts that will be connected to IB, and agreement on the specific conditions of IB.

5.3 Each IB User also has access to MB to the extent of the Authorisation and by using the IB Security Elements. Use of MB is conditional on access to IB.

5.4 At least one IB User must be specified for Main Client IB all the time.

5.5 The Client may at any time terminate the consent to the Third Party's access to the Services in the manner specified by the Bank.

6. Security

6.1 Services are secured against abuse using Security Elements.

6.2 To ensure secure access to Services the Bank may make use of Security Elements (e.g. a Cronto code, an SMS code etc.), and may collect and evaluate information relating to IB Users' access to Services. Actions for which authorization is given by an IB User are binding for the Client.

6.3 Each IB User may log in to Services and perform authorization either via a Cronto code, using a Token or e-Token, or via an SMS code.

In order to use SMS codes, an IB User must provide the Bank with a mobile phone number. In order to activate the Token or e-Token, the IB User must provide the Bank with an e-mail address or mobile phone number where activation codes will be sent.

An IB User may set up a PIN or Biometric Data (provided that their mobile device supports biometric reading) in order to access MB and make authorisations in MB. IB Users set up these Security Elements on their own directly in their MB.

The Bank has the right to (permanently or temporarily) restrict the range of methods available for authorization and/or the means used for obtaining them.

6.4 Data is automatically encrypted during transfer between the Client and the Bank.

6.5 Upon the provision of Services, the Security Elements will be provided, in the agreed manner, as follows:

(i) the IB Login Password will be provided only to the IB User, either in a secure envelope or via an email message;

(ii) the Token will be handed over in person either to the IB User or to a person authorised by the IB User;

(iii) the IB User may install an e-Token on his mobile device without restriction;

One Token or e-Token may not be used by more than one IB User.

6.6 An IB User may contact the Bank in the event that the Token does not function correctly. The Bank will arrange for the repair of the Token or its replacement with a new Token. The Bank provides the following warranties for Tokens:

(i) for Clients – consumers, the warranty period is two years,

(ii) for other Clients the warranty period is 6 months.

After the expiration of the warranty period, free of charge replacement of the Token will no longer be possible and in the event of an irreparable defect in the Token the Bank will sell the User or the Client a new Token.

6.7 There is a thirty-day time limit on the validity of the initial IB Login Password. Upon logging in to IB for the first time, the IB User is required to change the IB Login Password. IB Users will be denied access to Services after a specified number of incorrect attempts to enter an IB Login Password, Cronto code or SMS code.

6.8 Renewal of access may be requested by a Client or an IB User in person at a Place of Business, via the ELB channel, if this option is offered, or by phoning Customer Service.

6.9 Clients and IB Users using Services are obliged, in particular:

(i) to protect all Security Elements against abuse, loss, unauthorised disclosure and theft,

(ii) to change the IB Login Password provided by the Bank immediately after logging in for the first time.

6.10 Clients are also obliged to protect their own information system and its components against abuse and comply with applicable security measures described in the Security Principles.

6.11 Clients are responsible for duly securing Services against unauthorised access. Clients shall take measures to prevent the abuse of Services by third subject (different from the Bank or the Client).

7. Payment and banking services provided via Services

7.1 The main Payment and Banking Services available to IB Users via IB and MB are as follows:

(i) enter selected Payment Orders,

(ii) view balances on Accounts and the history of transactions performed on them, if any,

(iii) access Account statements,

(iv) access information relating to the Debit cards to which the Client has access via IB and MB,

(v) access other data and information available via IB and MB, and send authorised requests and messages to the Bank.

In IB and MB, IB Users may also set up notifications to be sent to them regarding Payment Transactions, changes in Account balances etc., and may make use of other available functions.

7.2 The following information can be obtained via the Account Information Service:

(i) a list of Payment Accounts connected to the Client's IB,

(ii) balances in the Payment Accounts connected to the Client's IB,

(iii) a list of Payment Transactions on the Payment Accounts connected to the Client's IB.

7.3 The Bank shall advise the Client of its intention to refuse to provide information on a Payment Account under Article 7.2; should this not be possible, the Bank shall notify the Client following the refusal without undue delay.

7.4 Payment Orders can be given for the Payment Accounts connected to the Client's IB via the Payment Initiation Service.

7.5 The conditions applying to the particular Payment and Banking Services provided via Services are defined in the GBC or respective SBCs; the use of the above services via Services and the other available functions of Services are described in detail in the IB and MB help section and/or the Bank's other related documents.

7.6 The Bank may change the scope of Payment and Banking Services provided via Services and the scope of Services functions at any time. The Bank shall inform the Client thereof.

7.7 Where Clients request the express performance of Domestic Orders in CZK to credit an account with another domestic Provider, they are obliged to specify this when submitting the Payment Order.

7.8 For Payment Orders manually entered into Services the Maturity Date is required information.

Where the import file so allows, the individual items in one bulk Payment Order imported into IB in a Batch can have different Maturity Dates and the payments can be performed from a single Client's different Accounts connected to IB. When importing a bulk Payment Order the IB User may select the immediately following Maturity Date, whereupon it will automatically be assigned the earliest possible Maturity Date for all items therein in accordance with the Business Conditions of PPF banka a.s. for Payments.

7.9 Payment Orders must be authorised at the latest as of their Maturity Date and within the time period for the submission of Payment Orders stated in the Business Conditions of PPF banka a.s. for Payments. If the authorization of Payment Orders is performed after this time period has expired, authorization will either be refused by the Service or the further processing of the Payment Orders will be refused after authorization.

7.10 In addition to the cases set out in the Agreement, the Bank can also refuse Payment Orders transmitted via the Payment Initiation Service in the following cases:

(i) suspicion of an unauthorised or fraudulent use of the Service or Security Elements,

(ii) the Initiated Payment Order was given through a person unauthorised to provide the Payment Initiation Service,

(iii) the Third Party providing the Payment Initiation Service has not proved its identity to the Bank in accordance with the Payments Act.

7.11 The Bank shall advise the Client and/or the IB User of its intention to refuse an Initiated Payment Order and the reasons for such refusal; should this not be possible, the Bank shall notify the Client of the reason for the refusal following the refusal without undue delay.

7.12 Clients and IB Users may contact Customer Service in the event of any problems with Services functions, with the authorization of Payment Orders and requests made to the Bank or other problems associated with Services.

8. Handling of Funds

8.1 Clients are responsible for ensuring that the Funds on an Account are handled via Services only by the IB Users.

8.2 Clients are obliged to inform the Bank of any changes in regard to IB Users, and to request a change of Services. Clients are liable for any loss or damage incurred due to the breach of this obligation.

9. Scope of access rights and IB Users' permissions

9.1 In an Authorisation, the Client can set up access rights and permissions for IB Users in accordance with the document Scope of Access Rights for the Internet and Mobile Banking of PPF banking a.s..

9.2 In an Authorisation, IB Users may be granted permission to authorise Payment Orders with the following scopes:

(i) **INDEPENDENTLY WITHOUT LIMIT** – an IB User performs the authorisation of Payment Orders independently without limitations.

(ii) **INDEPENDENTLY UP TO A SPECIFIED LIMIT** – an IB User performs the authorisation of Payment Orders independently up to the amount of a specified Limit. If Payment Orders exceed the specified Limit, IB Users may only enter them. Authorisation must be performed by an IB User who has been granted a higher Limit.

(iii) **INDEPENDENTLY UP TO A SPECIFIED LIMIT, BEYOND THE LIMIT JOINTLY WITH ANOTHER IB USER** – an IB User performs the authorisation of Payment Orders independently up to a specified Limit. Payment Orders exceeding the specified Limit must be authorised jointly with another IB User.

(iv) **JOINTLY WITH ANOTHER USER UP TO A SPECIFIED LIMIT** – an IB User performs the authorisation of Payment Orders only up to a specified Limit, and always jointly with another IB User.

(v) **JOINTLY WITH ANOTHER IB USER WITHOUT LIMIT** – an IB User always performs the authorisation of Payment Orders jointly with IB another User.

A permission to authorise with a different scope may also be set up following prior agreement with the Bank.

9.3 In an Authorisation, a Client may specify the following Limits for handling Funds on an Account:

(i) a Transaction Limit separately;

(ii) a Time-based Limit separately;

(iii) a Transaction Limit together with a Time-based Limit.

9.4 A Transaction Limit specifies the maximum possible amount of one Payment Order for which authorisation may be performed. Authorisation may be performed for an unlimited number of Payment Orders whose amounts do not exceed the Transaction Limit.

9.5 A Time-based Limit specifies the maximum possible aggregate value of Payment Orders for which authorisation may be performed in a designated time period. Authorisation may be performed for an unlimited number of Payment Orders provided that the aggregate amount of all such authorised Payment Orders does not exceed the Time-based Limit. A Time-based Limit may be set for one Business Day, one calendar week, calendar month or one calendar quarter. The Time-based Limit is reduced upon the authorisation of a Payment Order, and is then reset:

(i) at 00:00:01 a.m. each new Business Day, if the Time-based Limit is set for one Business Day. Payment Orders authorised outside of Business Days are deducted from the Time-based Limit of the next Business Day;

(ii) at 00:00:01 a.m. each Monday, if the Time-based Limit is set for a calendar week;

(iii) at 00:00:01 a.m. on the first day of each calendar month, if the Time-based Limit is set for a calendar month;

(iv) at 00:00:01 a.m. on the first day of each calendar quarter, if the Time-based Limit is set for a calendar quarter.

An exception is the cancellation of Payment Orders where the amount of the Payment Order being cancelled is not checked against the Time-based Limit.

9.6 If both a Transaction and a Time-based Limit have been set, both of these Limits must be adhered to at the same time, i.e. authorisation may be performed for a Payment Order whose amount does not exceed the set Transaction Limit and at the same time does not exceed the Time-based Limit. Therefore, if a Payment Order is within the Transaction Limit but the sum total of all Payment Orders for which authorisation has been performed to date exceeds the Time-based Limit, authorisation may not be performed for such Payment Order.

9.7 In the case of intrabank orders in foreign currency, SEPA Orders, and foreign orders (one-time and multiple), the Limit works with the relevant counter-value of the foreign currency in CZK converted using the current Exchange Rate at the time of their authorisation according to the rules specified in the GBC.

9.8 Payment Orders with a future Maturity Date are deducted from the respective Limits at the time of their authorisation.

9.9 Clients may arrange for Multiple or Multilevel Authorisation. Multilevel Authorisation may be arranged if the Client has also arranged Multiple Authorisation.

9.10 If Multiple/Multilevel Authorisation is arranged, authorisation by various IB Users according to the rules agreed in the Authorisation must be arranged for actions performed within the scope of Services.

9.11 IB Users always perform the authorisation of requests, messages and other communications sent to the Bank independently.

9.12 The Client can grant a different scope of access rights and permissions for each of the Services to an IB User.

10. Data transmission

10.1 Users may use Services at any time.

10.2 In justified cases, the Bank may interrupt the provision of Services, including the acceptance of Payment Orders. The Bank shall notify the Client of any scheduled downtime of Services via IB. In the event of technical faults on the part of the Bank or any third party, the Bank may interrupt the provision of Services without prior notice. Where the Client uses the Account Information Service and the Payment Initiation Service through a Third Party, the Bank shall advise the Client of any unavailability.

10.3 In order to access a Service, IB Users must always enter their IB Username and:

(i) if logging in using a Token or e-Token: enter their IB Login Password, scan the Cronto code and type in the generated authorisation code;

(ii) if logging in using an SMS code, enter their IB Login Password and the SMS code.

10.4 The only method by which an IB User may approve the performance of a Payment Order or request made to the Bank is its authorisation using a Cronto code or an SMS code.

10.5 The Bank accepts responsibility only for data received and confirmed by the Bank. The Bank is not liable for any damage incurred due to the incorrect or duplicated entry of data (Payment Orders or requests) via IB, MB or the Payment Initiation Service.

10.6 The Bank reserves the right to change the manner of submitting data, if required for the secure operation of Services or for other serious reasons.

11. Statements and complaints procedure

11.1 Clients are informed of Payment Transactions performed via Services in Account statements.

11.2 Clients and/or IB Users are also informed via IB, MB and the Account Information Service of all currently performed Payment Transactions and of the balance of the Funds on the Account.

11.3 The history of Payment Transactions is available in IB and MB for at least 13 months.

11.4 Clients may submit complaints relating to Services via IB, MB, Customer Service or at a Place of Business of the Bank.

11.5 Complaints may be submitted on behalf of a Client by any of its IB Users.

11.6 Complaints are settled in accordance with these SBC, the GBC and the Bank's Complaints Code.

12. Loss, abuse, faults and blocking of Services

12.1 Clients and IB Users are obliged to inform the Bank immediately if there is any suspicion of:

(i) the unauthorised disclosure of Security Elements,

(ii) the potential abuse of Services by a third party,

(iii) a program error and/or an error or abuse relating to the transmission or reception of data.

12.2 Clients and IB Users are also obliged, as soon as they discover any such occurrence:

(i) to report the loss or theft of Services or SW/HW enabling their use (in particular any Security Elements),

(ii) to report any unauthorised Payment Transaction for which they did not submit an order,

(iii) to request, where applicable, the blocking of Services for security purposes.

Such reports may be made in writing, in person at a Place of Business, via Customer Service or through the Call Centre.

12.3 The Client or the IB User, as applicable, agree that their telephone conversations with the Customer Service or the Call Centre will be recorded by the Bank or the Provider, stored and used as evidence in case of a dispute.

12.4 Following the making of a report as described above the Bank may block the use of Services. Clients and IB Users must cooperate effectively with the Bank during the performance of corrective measures proposed by the Bank.

12.5 Clients may request the Bank to provide written confirmation that the loss/theft/abuse of Security Elements was reported to the Bank; however, Clients must do so within 18 months of making a report according to Articles 12.1 or 12.2.

12.6 The Bank shall have the right to block the use of Services only for the following reasons:

(i) security of Services, in particular in cases of suspicion of unauthorised or fraudulent use of Services,

(ii) any significant increase in the risk that the Client will not be able to repay a loan that can be drawn through Services,

(iii) in the cases specified by applicable legal regulations.

Once the reasons for blocking Services cease to exist, the Bank shall unblock Services.

12.7 Prior to blocking Services or, if this is not possible, immediately thereafter, the Bank shall inform the Client of this restriction and the reason for it. This obligation shall not apply in the case that the provision of such information can frustrate the purpose of the restriction of Services or where this is contrary to legal regulations.

12.8 In the event that Clients find that access to Services has been blocked, they are obliged to take all necessary steps to unblock or restore their access without undue delay, in order to have access to Information that the Bank provides and/or discloses to them in accordance with the Payments Act.

13. Liability

13.1 The liability of Clients and of the Bank is provided for in the GBC, these SBC and the Agreement.

13.2 The Bank is not liable:

(i) for cases where Services cannot be used for reasons beyond the control of the Bank or its partners (interruption of the power supply, interruption of the connection with the Bank via public internet, strikes etc.) including any damage incurred as a result of such cases,

(ii) for damage incurred by the Client due to a breach of the Client's obligations set out in these SBC,

(iii) for damage incurred due to incorrect authorisation or any failure to perform a Payment Order for reasons on the part of the Client or on the part of a payment Beneficiary.

13.3 The electronic communications networks (public telephone lines, mobile networks, email and fax) used for communication between the Bank and Clients according to these Conditions are not under the direct control of the Bank, and the Bank is therefore not liable for any damage incurred by Clients due to their potential abuse. The protection of such networks and the confidentiality of messages sent via them must be ensured by the providers of the respective electronic communications services pursuant to legislation including, without limitation, Act No. 127/2005, on Electronic Communications, as amended.

13.4 The Bank is liable for the functioning and availability of Services, subject to compliance with the Agreement, the Security Principles, the Technical Requirements and any other instructions of the Bank.

13.5 If any malfunctioning of Services for reasons on the part of the Bank is discovered outside of the Bank's Business Hours, the Bank will commence work to rectify such malfunctioning on the next subsequent Business Day immediately after the beginning of the Bank's Business Hours.

13.6 Any and all information regarding Services and Payment and Banking Services provided via Services and their use is confidential, and Clients may not use such information in a manner contrary to the purpose for which it was provided to them.

13.7 The Client is also liable for any incorrectly entered data and technical faults on the part of the Client.

13.8 The Client is liable to the Bank for damage incurred by the Bank due to any breach of the Client's obligations under the Agreement, these SBC or the GBC, or as a result of any incorrect use of Services.

14. Termination of contractual relationship

14.1 The Agreement is discharged in cases specified in the GBC and also on the day of closing the Client's last Payment Account connected to IB.

14.2 In the event of the termination of the Agreement, access to Accounts via Services will be cancelled for all of the Client's Users:

(i) as at the date of termination of the Agreement for the transmission of Payment Orders via IB and MB and for the use of the Payment Initiation Service and Account Information Service,

(ii) one month after termination of the Agreement for the acquisition of Account information via IB and MB.

14.3 The Client's access to the Services that the Client uses through the Main Client will be terminated as of the day of the termination of the provision of Services to the Main Client.

15. Final provisions

15.1 These SBC come into force on 1 November 2022 and effect on 1 January 2023, as of which date they shall supersede the existing Business Conditions of PPF banka a.s. for Internet and Mobile Banking effective as of 1 July 2020.