BUSINESS CONDITIONS OF PPF BANKA A.S. FOR THE CLIENT API

Contents:

1. Introductory provisions

1.1 The Business Conditions of PPF banka a.s. for the Client API (hereinafter referred to as the "Conditions") lay down ground rules governing business relations between the Bank and its Clients in the use of the Client API Banking Service.

1.2 Unless otherwise provided by these Conditions, capitalised terms and expressions shall have the meaning assigned to them in the General Business Conditions of PPF banka a.s. (hereinafter referred to as the "**GBC**"). The terms and expressions thus defined shall apply mutatis mutandis to both the singular and plural.

1.3 These Conditions have been issued on the basis of and in accordance with Section 1751 of the Civil Code, the Payments Act, the Banking Act and, where appropriate, other related legislation.

1.4 These Conditions constitute "Specific Business Conditions" (hereinafter referred to as "**SBC**") issued in accordance with and further to the GBC. Relations between the Bank and the Client not regulated by these Conditions are governed by the GBC.

2. Definitions and rules of interpretation

2.1 Capitalised terms and expressions shall have the following meaning in these SBC:

API Administrator – a natural person authorised by the Client to manage the Client API, including but not limited to the configuration of the system, the administration of the Client Certificate, and communication with the Bank concerning the Client API. The API Administrator shall have access to IB set up in order to transmit messages and documents via a secure channel.

API – Application Programming Interface. This denotes an interface for secure machine communication and online data exchange.

Security Elements – the GBC define the following in particular as Security Elements: a Signing Certificate and Client Certificate.

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.

Certificate – the umbrella term for a Signing Certificate and Client Certificate.

Supplier – a third party that processes or provides services forming part of the Client API, or that contractually performs activities related to the operation of the Client API for the Bank.

Main Client – the client of the Bank through whom the Client uses, exclusively or in part, the Client API. The Client grants the Main Client and the Main Client's Users a power of attorney insofar as is strictly necessary for the Client to use the Client API through the Main Client.

Internet Banking (IB) – an online ELB system (operating via a permanent connection with the Bank) enabling a User to communicate with the Bank, to submit Payment Orders and requests to the Bank, and to obtain additional information, including information on Account balances and on any Payment Transactions in Accounts.

Client API – a special payment process for Clients who are not consumers to obtain information on Accounts and to place Payment Orders.

Client Certificate – a certificate enabling encrypted information to be received from the Bank via the Client API.

Limit – the total maximum amount of Account Funds available, as set in the form "Client API Access to Accounts". Limits, always set in CZK, may be set for a Payment Order (hereinafter referred to as the "Transaction Limit"), for a certain period of time (a Business Day, calendar week, calendar month or calendar quarter – hereinafter also referred to as the "Time-based Limit"), or combined for both a Payment Order and a certain period of time. A Limit shall be the aggregate for all Accounts, as listed in the Client API Access to Accounts, that the User may manage via the Client API.

Signing Certificate – a certificate needed to authorise Payment Orders placed with the Bank via the Client API.

Client API Access to Accounts – a form, provided by the Bank, that has the requisites of a power of attorney and is used by the Client to set the scope of access rights, in particular regarding access to Accounts, as well as the placing and, where appropriate, authorisation of a Payment Order.

Agreement – an agreement, regardless of how it is titled, between the Client and the Bank under which the Client is allowed to use ELB.

Technical Requirements – a set of software and hardware requirements necessary to ensure the functioning of the Client API on the part of the Client. The Bank publishes the current wording of Technical Requirements on its Website. Technical Requirements do not constitute Information within the meaning of the GBC.

API User – an Authorised Party authorised by the Client to manage the Client's Accounts and identified by the Bank within the meaning of Act No. 253/2008. The scope of authorisation is set out in the Client API Access to Accounts. In relation to the Services used by the Client through the Main Client, the Main Client's API User is regarded as the Client's API User.

Customer Service – a telephone number or email address used to report faults or irregularities in the Client API and to provide user support to Clients and API Users. The Customer Service's Business Hours are available on the Bank's Website.

2.2 Unless otherwise provided by these SBC, capitalised terms and expressions shall have the meaning assigned to them in the Agreement.

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 shall provide the Client API under an Agreement or further to a request from the Client and the acceptance thereof by the Bank.

3.2 The Client may use the Client API only for the agreed purpose.

3.3 The Client API may be used solely in connection with Accounts that are accessible via the Client's Internet Banking.

4. Technical requirements

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

4.2 The Bank shall be entitled to improve the Client API from time to time by upgrading to a higher version; the Bank shall inform the Client of any such planned upgrade sufficiently in advance of performing the upgrade.

4.3 The Client shall ensure that it has hardware that is adequate in terms of its functioning and performance and that any other installed software is compatible with the Client API for the entire period of validity of the Agreement. In the event of improvements and/or upgrades, the Client shall ensure that it has the technical equipment to accommodate such a change.

4.4 By signing the Agreement or by submitting the documents specified by the Bank for the provision of the Client API, the Client guarantees that it is technically prepared for the use of the Client API to the extent of the Technical Requirements.

5. Client API implementation

5.1 The Bank shall provide the Client API to the Client only if the Client holds at least one Payment Account with the Bank and has set up Internet Banking.

5.2 The Bank shall provide the Client with access to use the Client API on the basis of a concluded Agreement or by accepting a request for the provision of the Client API, the appointment of an API Administrator and, where appropriate, an API User, a specification of the Accounts that will be connected to the Client API, and agreement on the specific conditions of the Client API.

5.3 The API Administrator and the API User may be one and the same person.

5.4 The API Administrator and the API User shall also have access to the IB to ensure secure communication and the transmission of the necessary information regarding the Client API.

6. Security

6.1 Security Elements secure the Client API against misuse.

6.2 To ensure secure access to the Client API, the Bank may make use of Security Elements and may collect and evaluate information relating to the use of the Client API.

6.3 If the Client is to submit Payment Orders to the Bank via the Client API, the Client shall designate, as the person authorised to do this, only an API User, who shall arrange for the submission of Payment Orders to the Bank on the part of the Client. Payment Orders submitted to the Bank by this person shall be regarded as Payment Orders submitted and authorised by the Client. The Bank shall not be liable for any damage caused by non-payment as a result of the submission of incorrect, incomplete or otherwise damaged Payment Orders. Actions authorised by the API User's Signing Certificate shall be binding on the Client.

6.4 Data shall be automatically encrypted during transmission between the Client and the Bank.

6.5 Upon provision of the Client API, Certificates shall be delivered to the API Administrator and the API User via IB.

6.6 The Certificates shall be valid for one year from the date on which they are generated by the Bank and sent to the Client. Before this period expires, the API Administrator and the API User shall apply, via IB, for new Certificates to be generated.

6.7 The Client, the API Administrator and the API User shall, in particular:

(i) protect all Security Elements against misuse, loss, unauthorised disclosure and theft;

(ii) protect their own information system and components thereof against misuse.

6.8 The Client shall be responsible for duly securing the Client API against unauthorised access. The Client shall take measures to prevent the misuse thereof by third parties (parties other than the Bank or the Client).

7. Payment and Banking Services provided via the Client API

7.1 The Client may use, in particular, the following Payment and Banking Services via the Client API:

(i) place selected Payment Orders;

(ii) obtain balances of the Accounts and the history of transactions made in them.

7.2 The conditions for individual Payment and Banking Services provided via the Client API are set out in the GBC or in the relevant SBC. Details of the use of such services via the Client API and other available functionalities are described in the Technical Requirements, in the Swagger API for secure communication with Clients, and, where appropriate, in other related documents of the Bank.

7.3 The Bank shall be entitled to modify the scope of Payment and Banking Services provided via the Client API, and the scope of the Client API's functionality, at any time. The Bank shall notify the Client thereof.

7.4 In addition to the cases set out in the Agreement, the Bank may also refuse a Payment Order submitted via the Client API if it suspects unauthorised or fraudulent use of the Client API or Security Elements.

7.5 The Client or the API Administrator may contact the Customer Service if there are problems with the functionality of the Client API or other problems related to the Services.

8. Scope of access to Accounts and handling of Funds

8.1 The Client may establish Account access only for information to be obtained, only for Payment Orders to be submitted, or for both simultaneously.

8.2 Authorisation may be set for the submission of Payment Orders to the following extent:

(i) **NO LIMIT** – Payment Orders may be submitted with no Limit on their amount.

(ii) **UP TO A SPECIFIED LIMIT** – Payment Orders may be submitted only up to a specified Limit. The Bank will not process Payment Orders that exceed the set Limit.

8.3 The Client may set the following Limits for the handling of Funds in Accounts:

(i) a Transaction Limit on its own;

(ii) a Time-based Limit on its own;

(iii) a Transaction Limit and a Time-based Limit.

8.4 A Transaction Limit specifies the maximum possible amount up to which one Payment Order may be authorised. An unlimited number of Payment Orders may be authorised provided that their amounts do not exceed the Transaction Limit.

8.5 A Time-based Limit specifies the maximum possible aggregate value of Payment Orders that may be authorised in a designated period of period. An unlimited number of Payment Orders may be authorised 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, one calendar month or one calendar quarter. The Time-based Limit shall be reduced upon authorisation of a Payment Order and shall then be reset:

(i) at 00:00:01 a.m. each Business Day if the Time-based Limit is set for one Business Day. Payment Orders authorised outside Business Days shall be 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.

8.6 If both a Transaction Limit and a Time-based Limit have been set, both of these Limits shall be adhered to at the same time, i.e. a Payment Order may be authorised if its amount does not exceed the set Transaction Limit and if, at the same time, it 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 that have been authorised to date exceeds the Time-based Limit, such a Payment Order cannot be authorised.

8.7 In the case of Intrabank Orders in Foreign Currency, SEPA Orders, and Foreign Orders, the Limit shall include the corresponding equivalent of the foreign currency in CZK converted using the current Exchange Rate prevailing at the time of their authorisation according to the rules specified in the GBC.

8.8 Payment Orders with a future Maturity Date shall be deducted from the respective Limits at the time of their authorisation.

8.9 The Bank shall not be liable for any damage caused by non-payment as a result of the submission of incorrect, incomplete or otherwise damaged Payment Orders.

9. Data transmission

9.1 API Users may use the Client API at any time.

9.2 In justified cases, the Bank shall be entitled to interrupt the provision of the Client API, including the acceptance of Payment Orders. The Bank shall notify the API Administrator and API Users of any scheduled Client API downtime via Internet Banking. If there are technical faults on the part of the Bank or any third party, the Bank shall be entitled to interrupt the provision of the Client API without prior notice.

9.3 The Bank shall be liable only for data received and confirmed by the Bank. The Bank shall not be liable for any damage incurred due to the incorrect or duplicated placing of Payment Orders via the Client API.

9.4 The Bank reserves the right to change the data transmission method if required for the secure operation of the Client API or for other serious reasons.

10. Statements and complaints procedure

10.1 The Client shall be informed of Payment Transactions performed via the Client API in Account statements.

10.2 The history of Payment Transactions shall remain accessible in the Client API for 13 months.

10.3 The Client may lodge complaints relating to Services via Internet Banking, the Customer Service or at a Place of Business of the Bank.

10.4 Complaints may be lodged on behalf of the Client by the API Administrator or an API User.

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

11. Loss, misuse, faults and blocking of the Client API

11.1 The Client and the API Administrator shall inform the Bank immediately of any suspicion of:

(i) the unauthorised disclosure of Security Elements;

(ii) the potential misuse of the Client API by a third party;

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

11.2 Without undue delay after discovering such an occurrence, the Client and the API Administrator shall also:

(i) report the loss or theft of the Client API or means enabling the use thereof (including, but not limited to, Security Elements);

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

(iii) request, where applicable, the blocking of the Client API for security reasons.

Such reports may be made in writing, in person at a Place of Business of the Bank, or via the Customer Service. Where a report is made via the Customer Service, the reporting person shall provide contact details, via which the Bank will verify the information provided. The Bank may refuse to perform the requested action if it is not possible to verify the information provided.

11.3 After the aforementioned report has been made, the Bank shall be entitled to disable the use of the Client API. The Client shall cooperate effectively with the Bank in the implementation of corrective measures proposed by the Bank.

11.4 The Client may request written confirmation from the Bank that the loss/theft/misuse of Security Elements has been reported to the Bank, but must do so within 18 months of making a report pursuant to Articles 12.1 and 12.2.

11.5 The Bank shall be entitled to block the use of the Client API only for the following reasons:

(i) the security of the Client API, in particular if unauthorised or fraudulent use of the Client API is suspected;

(ii) a significant increase in the risk that the Client will be unable to repay credit that can be drawn via the Client API;

(iii) in cases foreseen by applicable legislation.

Once the reasons for blocking the Client API pass, the Bank shall unblock it.

11.6 Prior to blocking the Client API 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 if the provision of such information could frustrate the purpose of restricting the Client API or where this would be unlawful.

11.7 Upon discovering that access to the Client API has been blocked, the Client shall take all steps required to unblock or restore access without undue delay in order to have access to Information that the Bank Provides and/or Discloses to the Client in accordance with the Payments Act.

12. Liability

12.1 The liability of the Client and of the Bank shall be governed by the GBC, these Conditions and the Agreement.

12.2 The Bank shall not be liable:

(i) for cases where the Client API 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 Conditions;

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

12.3 The electronic communications networks (public telephone lines, mobile networks, email and fax) used for communication between the Bank and the Client pursuant to these Conditions are not under the direct control of the Bank, and the Bank is therefore not liable for any damage incurred by the Client due to any misuse thereof. The protection of such networks and the confidentiality of messages sent via them shall 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.

12.4 The Bank shall be liable for the functioning of the Client API, subject to compliance with the Agreement, Security Principles, Technical Requirements and any other instructions of the Bank.

12.5 If any malfunctioning of the Client API for reasons on the part of the Bank is discovered outside the Bank's Business Hours, the Bank shall commence work to rectify such malfunctioning on the next Business Day immediately after the beginning of the Bank's Business Hours.

12.6 Any and all information regarding Services and Payment and Banking Services provided via the Client API and their use shall be confidential, and the Client may not use such information in a manner contrary to the purpose for which it was provided to the Client.

12.7 The Client shall also be liable for any incorrectly entered data and technical faults on the part of the Client.

12.8 The Client shall be liable to the Bank for damage incurred by the Bank due to any breach of the Client's obligations under the Agreement, these Conditions or the GBC, or as a result of any incorrect use of the Client API.

13. Termination of contractual relationship

13.1 The Agreement shall be terminated in cases specified in the GBC and also on the date on which the Client's last Payment Account connected to Internet Banking is closed and/or on which Internet Banking is terminated.

13.2 If the Agreement is terminated, access via the Client API shall be:

(i) cancelled immediately for the submission of Payment Orders;

(ii) cancelled one month after termination of the Agreement for the acquisition of Account information.

13.3 The Client's access to the Client API that the Client uses through the Main Client shall be terminated as at the date of termination of the provision of the Client API to the Main Client.

14. Final provisions

14.1 These Conditions shall enter into force on 1 May 2021 and take effect on 1 July 2021 as of which date they shall supersede the existing Business Conditions of PPF banka a.s. for Client API effective as of 1 January 2021.