

**BUSINESS CONDITIONS OF PPF banka a. s.
FOR THE USAGE OF INTERNETBANKING SERVICES****INTRODUCTORY PROVISIONS**

1. The Bank's Business Conditions for the Usage of Internetbanking Services (hereinafter the "Conditions") stipulate the basic rules which are applied to business relations between the Bank and its Clients during the use of the Banking Service IB for CA.
2. Where terms or phrases starting with an uppercase letter are used in these Conditions, they shall have the meaning stipulated in the article Definition of Terms in the General Business Conditions of PPF Banka a.s. (hereinafter the "GBC") and/or Definition of Terms hereof, or the meaning specified in the individual provisions hereof. These defined terms and phrases shall be used analogically in single and plural form.
3. The Conditions are issued based on and in accordance with the provisions of Section 273, Commercial Code, the Payments Act, the Banking Act and other potential related legal regulations.
4. These Conditions are the so-called Specific Business Conditions (hereinafter "SBC") issued in accordance with and following up on the GBC. The relations between the Bank and Client not regulated by these Conditions are governed by the GBC.
5. These Conditions are an integral part of the Agreement on IB; concluded between the Client and the Bank. If the Agreement on IB contains provisions that differ from these Conditions, the provisions of the Agreement on IB shall take precedence. If these Conditions contain provisions that differ from the provisions of the GBC, these shall take precedence over the provisions of the GBC.

DEFINITION OF TERMS

1. **Authorisation** – a process during which the User gives consent to the order or instruction for the Bank using the Electronic Signature or SMS code.
2. **Authorisation Right** – a rule which authorises the User to view to selected CA from the List of Accounts, enter Payment Orders or instructions from the individual CA for the Bank within the framework of the stipulated Limit and to Authorise Payment Orders or instructions for the Bank. The Authorisation Right also stipulates the manner of Authorisation.
3. **Security Elements** – according to the GBC, these are in particular – the Certificate, Electronic Signature, PIN, IB Login Password, SMS code, Token and IB Username.
4. **CA** – a current account.
5. **Certification Centre** – the internet application of the registration authority for certifying Electronic Signatures; ensures the creation of new and renewal of existing Certificates.
6. **Certificate** – a personal certificate generated by the Certification Centre, which verifies the User's identity.

7. **Batch** – the import of one bulk Payment Order in the form of a file (generated e.g. by the Client's account system) in a specific format.
8. **Supplier** – a third party that is to process or ensures services forming part of the IB, or which ensures activities related to IB operation for the Bank based on a contractual relation.
9. **Electronic Signature** – encrypted data in electronic form, which is attached to submitted data.
10. **IB (also Internetbanking)** – an electronic Payment Instrument and also Banking Service, through which the User is enabled to communicate with the Bank, submit Payment Orders and instructions to the Bank, obtain additional information including information about the balance on the CA and Payment Transactions performed on it.
11. **Limit** – is the total maximal amount of Monetary Funds for handling of the Monetary funds on the CA by the User. The Limit is always stipulated in CZK, is assigned to the specific User and may be set for a Payment Order or Batch (also referred to as the "Transaction Limit"), for a certain time period (day, week or month – also referred to as the "Time Limit"), or in combination for the Payment Order/Batch and also for a certain time period. The Limit applies in total to all CAs which the User can handle via IB.
12. **Rights** – the summarised term for the Authorisation Right and Viewing Right. Granted Rights form an annex to the Agreement on IB.
13. **PIN (Personal Identification Number)** – the code for access to the Token on which the Certificate is stored. The PIN must have six to twenty characters, may contain only alphanumeric characters without diacritical marks, of which minimally one uppercase letter, minimally one lowercase letter and minimally one digit.
14. **Viewing Right** – a rule that authorises the User to view selected CA from the List of Accounts, or enter orders or instructions from individual CA for the Bank for Authorisation. Viewing Right does not authorise the User to Authorise orders and instructions for the Bank, not even when paired with a User with Authorisation Right.
15. **IB Login Password** – the password is granted to the User in the event of choosing Authorisation via SMS code, which the User enters when logging into IB along with the IB Username . The IB Login Password must have six to ten characters, may contain only alphanumeric characters without diacritical marks, of which minimally one uppercase letter, minimally one lowercase letter and minimally one digit and must not be repeated.
16. **List of Accounts** – contains a list of the CA, which can be viewed or which can be handled via IB; this List of Accounts forms an annex to the Agreement on IB.

17. **Agreement on CA** – the Agreement on the Current Account concluded between the Bank and the Client.
18. **Agreement on IB** – Contract on Internetbanking concluded between the Bank and the Client.
19. **SMS code** – an eight-digit numerical unique identifier, which is sent to the User to the chosen domestic mobile telephone number. It is generated separately for:
 - each login to IB and serves to verify the User,
 - each Payment Order or instruction for the Bank and serves for its Authorisation.
 It is not an encrypted signature.
20. **Token** – the USB equipment for placement and storage of the Certificate.
21. **User** – a natural person authorised by the Client in the Rights to use IB actively, i.e. in particular to handle the Monetary Funds on the Client's CA and to Authorize orders or instructions for the Bank and to send Authorized messages to the Bank.
22. **User Guide** – a set of the Bank's rules for use of IB. The Bank is entitled to amend the User Guide. The current version of the User Guide shall be published by the Bank on its Website. The User Guide does not constitute Information in the meaning of the GBC.
23. **IB Username** – the User's username for IB, which the Client and Bank agree on and which is indicated in the annex to the Agreement on IB. The IB Username must have eight to sixteen characters, may contain only alphanumeric characters without diacritical marks, of which at least one uppercase letter, at least one lowercase letter and at least one digit.
24. **Multiple Authorisation** – a setting during which securing of the selected number of User Authorisations (2 or more) is required for usage of IB.
25. **Multilevel Authorisation** – a setting during which securing of the selected number of User Authorisations (1 or more) according to the stipulated Limit for usage of IB.
26. **Customer Service** – the telephone number or e-mail address that is used for reporting of faults or discrepancies in IB and for providing of user support to Clients and Users. The telephone number is available on Business Days from 8:00 to 17:00, the e-mail address is available non-stop.

GENERAL PROVISIONS

1. IB is established upon the conclusion of an Agreement on IB between the Client and the Bank. The legal relations related to the IB are governed by the law of the Czech Republic.
2. The Client and User are bound to become familiar with the Agreement on IB, the Conditions, the User Guide, the Security Principles and the GBC and undertake to adhere to them. The Client always bears full liability for violation of the conditions stated at all above mentioned documents by the Users.
3. If the User is not the Client, it is necessary that he/she grants the Bank express consent to personal data processing in accordance with GBC prior to assigning to the Rights. Should a User fail to grant

the Bank this express consent, the Bank is authorized not to assign him/her the Rights.

4. Remunerations and fees for tasks related to the usage of IB are charged from CA by the Bank in the amount according to the Bank's Pricelist valid on the day of charging the fee, eventually in the individual amount agreed in the Agreement on IB, regardless of whether the transfer sum is covered by the available Monetary Funds on the CA.
5. In the List of Accounts, the Client stipulates the basic CA, to the debit of which the prices for IB establishment and administration and prices for other services related to IB provision shall be charged. This CA is opened preferably in CZK; it may be opened in a currency other than CZK only if the Client does not have any account in CZK opened at the Bank.
6. Other prices, remunerations and fees related to Payment Transactions and Banking Services are charged from the CAs through which the Payment Transaction was performed, or the Banking Service provided.
7. The Client accesses IB through the Website. The Client may use IB only for the agreed purpose. The Client uses IB through the Users.
8. Client acknowledges that, within the relevant Rights, Users have access to the information on the balance and transactions on the CA that they operate.
9. Performance of payments via IB is governed by the GBC, unless these Conditions or the Agreement on IB stipulate otherwise.

I. TECHNICAL REQUIREMENTS

1. **Software (SW):** internet browser; MS Internet Explorer version 6.0 and higher and Mozilla/Firefox version 3.0 and higher are supported.
When logging in using the Electronic Signature with Certificate, the following are also required:
 - SW Token PKI Client – application for Token management; this SW is supported by OS Windows XP and higher,
 - SW Java RunTime, version 1.5 and higher,
 - BSC applet for communication with the Token.
 When submitting Payment Orders in the form of Batches, it is also necessary to have SW that generates the batch file in CSV format or Gemini 4.1 format.
2. **Hardware (HW):** PC or other computer technology system connected to the internet.
3. The Bank is authorised to perfect IB by means of upgrades to a higher version; the Bank is obliged to inform the Client of planned upgrades sufficiently in advance before upgrading to the higher version.
4. The Client is obliged to ensure adequate HW in functional and performance terms, and the compatibility of other installed SW with IB throughout the validity of the Agreement on IB, whereas in the event of improvement and/or upgrade to a higher IB version, the Client is obliged to ensure the appropriate technical equipment.
5. By signing the Agreement on IB, the Client guarantees its technical readiness for IB usage.

II. SERVICE IMPLEMENTATION

1. The Bank shall conclude an Agreement on IB with the Client only if the Client has opened at least one CA with the Bank.
2. The Bank makes the IB accessible for usage by the Client based on the signing of the Agreement on IB and after handover of the respective annexes to the Agreement on IB, duly completed and signed by the Client and Users, if applicable.
3. When signing the Agreement on IB, the Client stipulates the List of Accounts, Users, their Rights, manner of Authorisation and Limits. The Client may change these settings at any time in writing at the Place of Business.
4. If the Client cancels the CA that is indicated in the List of Accounts as the basic CA, the Client is obliged to stipulate a new basic CA from the List of Accounts.

III. SECURITY

1. To ensure secure access to IB, the Bank uses in particular a public key infrastructure (PKI), which fulfils the requirements to ensure all the security demands by means of asymmetric encryption, User identity verification using a Certificate and an Electronic Signature as a means of data undeniability and integrity. To ensure secure access to IB, the Bank is authorised to use other Security elements (e.g. SMS code) and further to collect and assess information related to Users' access to IB. Actions Authorised by the authorised User are binding for the Client. The Bank is authorised to condition the use of Authorisation with additional Security elements.
2. Each User may log in to IB and perform Authorisation in one manner only, either via SMS code or via Electronic Signature.
3. Data are automatically encrypted during the transfer between the Client and the Bank.
4. After signing the Agreement on IB, the User shall be handed over in the agreed manner according to the chosen means of Authorisation under this Agreement the following:
 - Authorisation via SMS code – IB Login Password shall be handed over in person or sent via post to the User in a sealed envelope, or sent to the User via SMS message to the domestic mobile operator number designated for sending SMS codes,
 - Authorisation via Electronic Signature – the Token shall be handed over in person to the Client, a sealed envelope with the Certification Centre Login Name and a sealed envelope with the Certification Centre Login Password shall be handed over in person or sent via post to the User.
5. In the case of Authorisation via Electronic Signature, the Bank shall sell the Client a separate Token for each User. The Token serves exclusively to store the Certificate necessary for access to IB and for Authorisation of Payment Orders and instructions for the Bank. The User is not authorised to use the Token for any other purpose or for the storage of User's data.

6. SW for operation of the Token is available free in the Certification Centre, and the User is obliged to download and save this SW to User's PC before first using the Token.
7. The Bank provides a two-year warranty on the Token. If the Token is dysfunctional, the Client or User may address the Bank. The Bank shall ensure repair of the Token or its replacement with a new one. After the warranty period, free of charge replacement of the Token is no longer possible and in the event of an irreparable flaw, the Bank shall sell the Client a new Token.
8. The Certificate is valid for one year. The User is obliged to ask for generating of a new Certificate in the Certification Centre before this validity period expires. If the User does not ask for generating of a new Certificate within the given time period, the User shall be denied access to IB.
9. The validity of the IB Login Password and PIN is not time-limited. However, the Bank recommends that the Users change the IB Login Password and PIN at least once a year.
10. Access to IB shall be denied to the User also after the stipulated number of incorrectly entered PINs (in the case of logging in and Authorisation via Electronic Signature) or the IB Login Passwords (in the case of logging in and Authorisation via SMS code).
11. Renewal of access must be requested in person by the Client at the Place of Business only.
12. The Client and User using IB are particularly obliged:
 - To protect all Security Elements against abuse or against their loss, disclosure or theft,
 - To change the IB Login Password provided by the Bank (if Authorisation via SMS code was chosen) immediately after logging into IB for the first time,
 - To change the PIN (if Authorisation via Electronic Signature was chosen) before first use of IB; the SW for operating the Token provided by the Certification Centre must be used to make this change.
13. The Client is also obliged to protect Client's own computer technology system and the components thereof against abuse.
14. The Client is responsible for due securing of the IB against unauthorised intervention. The Client shall undertake such measures so as to prevent abuse of the IB by a third party.
15. The Client and user are obliged to use only the SW provided by the Certification Centre to operate the Token. The Bank shall bear no liability for any damages arising from the use of different SW to operate the Token, or use of the Token for purposes other than accessing IB and Authorisation of orders and instructions for the Bank. The Bank shall likewise bear no liability for abuse of the Token by using the preset PIN, and damages related to this abuse, if the User failed to change the PIN immediately after the first sign-on to IB.

IV. BANKING SERVICES PROVIDED VIA IB AND OTHER IB FUNCTIONALITIES

1. The User may use the following Banking Services in particular via IB:
 - domestic one-off payment/transfer orders,
 - domestic bulk payment/transfer orders,
 - domestic one-off orders for direct debit,
 - domestic standing payment/transfer orders,
 - transfers within the Bank in foreign currencies,
 - Foreign Payment Orders.
2. If the Client requests express performance of Payment Order carrier to the credit of an account with another domestic Provider, he/she is obliged to indicate this request in the relevant field in the course of entering the Payment Order to IB.
3. The conditions for the individual Banking Services provided via IB are defined in the GBC or respective SBC.
4. The User may view the balances of CA, history of Payment Transactions performed on CA, check other data and information available via IB and send Authorised messages to the Bank.
5. The Bank is authorised at any time to adjust the Scope of Banking Services provided via IB and the scope of IB functionality.
6. In the event of problems with IB functionality, with Authorisation of orders or instructions for the Bank or other problems related to IB, the Client or User may contact Customer Service.

V. AUTHORISATION AND VIEWING RIGHTS

1. The User may be granted one of the following Authorisation Right:
 - **INDEPENDENT (also marked "S")** – the User with this Authorisation Right Authorises orders and instructions for the Bank independently without limitation,
 - **INDEPENDENTLY UP TO THE DESIGNATED LIMIT (also marked "A")** – the User with this Authorisation Right Authorises orders and instructions for the Bank up to the stipulated Limit independently. Orders and instructions that exceed the stipulated Limit may only be placed by the User with this Authorisation Right into the IB. Authorisation must be performed by a User with superior Authorisation Right or a User with a higher Limit.
 - **INDEPENDENTLY UP TO THE DESIGNATED LIMIT, BEYOND THE LIMIT JOINTLY WITH ANOTHER USER (also marked "B")** – the User with this Authorisation Right Authorises orders and instructions for the Bank up to the stipulated Limit. Orders and instructions for the Bank beyond the stipulated Limit must be Authorised jointly with another User with superior Authorisation Right or a User with a higher Limit,
 - **JOINTLY WITH ANOTHER USER (also marked "C")** – a User with this Authorisation Authorises orders and instructions for the Bank always jointly with another User.
2. A User with Authorisation Right is an Authorised Party in the meaning of the GBC.

3. The User may be granted one of the following Viewing Right:
 - **PASSIVE (also marked "P")** – a User with this Viewing Right may only view the CA and may only place orders and instructions for the Bank. A User with Authorisation Right must Authorise orders and instructions for the Bank.
 - **VIEWING (also marked "V")** – a User with this Viewing Right may only view the CA, the User does not have the right to place or Authorise orders or instructions for the Bank.
4. The User may be granted the same Rights for all CAs or different Rights for each CA.
5. If Multiple/Multilevel Authorisation is arranged, User Authorisation according to the rules agreed in the Rights must be ensured for actions within IB.

VI. HANDLING OF MONETARY FUNDS

1. The Client is liable for ensuring that the Monetary Funds on the CA will be handled via IB only by the Users listed in the Rights, in the manner defined in the Authorisation Right.
2. The Client is obliged to inform the Bank of any changes concerning the Users and request a change in the annexes to the Agreement on IB in which the changes occurred. The changes thus performed are effective on the Business Day following the day of submission of the duly signed annexes to the Bank, unless agreed otherwise between the Bank and the Client. The Client is responsible for any damages resulting from the breach of this obligation.
3. In the Agreement on IB, the Client may arrange Multiple/MultiLevel Authorisation. The condition of arranging Multilevel Authorisation is that the Client has agreed Multiple Authorisation at the same time. The setting of the respective Authorisation Right is an essential condition for the User to be authorised to perform Authorisation.
4. When arranging Multiple/Multilevel Authorisation, it is necessary for handling the Monetary funds on the CA in excess of the User's Limit that the respective Payment Order be additionally Authorised by the number of Users with the respective Authorisation Right as stipulated in the Agreement on IB.
5. In the Authorization Right, the Client may stipulate Limits for handling Monetary Funds on the CA.
6. The Transaction Limit stipulates the maximal possible amount of one Payment Order, or the maximal total sum of one Batch, up to the value of which the User may Authorize Payment Orders or a Batch. The User may Authorize an unlimited number of Payment Orders, the sum of which will not exceed the Transaction Limit or record an unlimited number of Batches if the total sum of each of the batches does exceed the Transaction Limit.
7. The Time Limit stipulates the maximal possible total amount of Payment Orders and Batches, which the User can Authorize in the designated time period. The User may Authorize an unlimited number of Payment Orders and Batches, if the total amount of all such Authorized Payment Orders and Batches does not exceed the Time Limit. The Time Limit may be set for the period of one Business Day, one calendar

week and one calendar month. The Time Limit is reduced at the moment of Payment Order Authorization and is renewed:

- If the Time Limit for a Business Day is set at 00:00:01 on every Business Day. Payment Orders and Batches Authorized outside of Business Days are deducted from the Time Limit of the following Business Day;
 - If the Time Limit for a calendar week is set at 00:00:01 on a Monday,
 - If stipulating a Time Limit for a calendar month is set at 00:00:01 on every first day of the calendar month.
8. If a Transaction and Time Limits are stipulated for the User, both of these Limits must be observed simultaneously. This means that the User can Authorize a Payment Order, the amount of which does not exceed the set Transaction limit, and at the same time does not exceed the Time Limit, i.e. if the Payment Order fulfils the Transaction Limit but the total of all Authorized Payment Orders to date exceeds the Time Limit, such Payment order cannot be Authorized. The same applies for Batches.
9. In the case of an transfer within the Bank in a foreign currency and a Foreign Payment Order, the respective counter-value of the foreign currency in CZK at the moment of their Authorization (converted using the current Exchange Rate according to the rules stipulated in the GCB) is included into the Limit.
10. Payments with future maturity are deducted from the respective Limits at the moment of the Authorization the Payment Order or the Batch.
11. If Payment orders are submitted to the Bank via a Batch and the Client's CA does not have sufficient funds to perform all the Payment Orders at once, the Bank shall perform the Payment Orders up to the value of the available funds on the CA, in the order designated by the Bank.

VII. SUBMISSION OF DATA

1. Users can use IB twenty-four hours a day, seven days a week. In justified cases, the Bank is authorised to interrupt IB service provision, including the acceptance of Payment Orders. The Bank usually informs of the planned interruption of availability in advance, generally via IB. In the case of technical flaws on the part of the Bank or any third party, the Bank is authorised to interrupt IB provision even without prior notice.
2. For access to IB, the User is always obliged to enter the IB Username and also:
 - if logging in using a Token: record the Certificate and enter the Token PIN,
 - if logging in using an SMS code: the IB Login Password and the SMS code.
3. The Maturity Date for Payment Orders and Batches entered via IB is mandatory information. If a Payment Order or a Batch contains an earlier Maturity Date than the date of Payment Order or Batch Authorization, then IB does not allow Authorization of such a Payment Order or Batch. The other conditions, deadlines for submission of orders and instructions to the Bank, their processing, recalling of

Payment Orders, or rejection of a Payment Order by the Bank are defined in the GBC.

4. The only means by which the User consents to the performance of an order or instruction to the Bank is its Authorisation via Electronic Signature or SMS code.
5. The Bank is liable only for data received and confirmed by the Bank. The Bank is not liable for potential damages caused by incorrect or duplicated data entry (Payment Orders) via IB.
6. The Bank reserves the right to change the manner of submitting of data, if required for the secure operation of IB or other substantial reasons.

VIII. STATEMENTS AND COMPLAINTS

1. The Client is informed of Payment Transactions via IB in a CA statement delivered by the way arranged in the Agreement on CA.
2. The Client and/or User is also informed through IB of all currently performed Payment Transactions and of the balance of Monetary Funds on the CA.
3. By course of the Banking Act, the Bank keeps the internal records allowing the tracing of Payment Transactions and correction of errors.
4. The Client and Users are obliged to control periodically whether the data of Payment Transactions correspond to the entered Payment Orders and whether the entered Payment Orders were performed or rejected by the Bank. The Client and Users are also obliged to report the found flaws in Payment Order statements or errors or other discrepancies in CA administration to the Bank without undue delay. Late reporting of damage may result in the expiry of the Client's claim for damages
5. The Client may make claims related to IB via Customer Service or at the Place of Business.
6. The Client agrees that all telephone calls made by the Client or by a User through Customer Service are recorded and that the Bank is authorized to use such a sound recording as a reference for potential settling of claims.
7. Any User may make the claim on behalf of the Client.
8. Complaints are settled according to these Conditions, the GBC and the Bank's Complaints Code.

IX. LOSS, ABUSE, BREAKDOWNS AND BLOCKING OF IB

1. The Client and Users are obliged to inform the Bank immediately if there is any suspicion of:
 - disclosure of Security Elements or the possibility of abuse of IB by a third party,
 - a programme error or error or abuse concerning the sending or reception of payments, Electronic Signature, Certificate, IB Login Password and/or SMS code.
2. The Client and Users are also obliged to report immediately upon ascertainment:
 - any loss or theft of the IB or facilities that enable its use,

- any unauthorised Payment Transaction to which they did not give an order,
- potentially request the blocking of IB for security reasons.

The respective report may be performed in writing, in person at the Place of Business or via telephone or electronic mail through Customer Service. If the report is performed via Customer Service, the reporting person must provide return contact information to which the Bank will perform verification of the sent data. If the sent data cannot be verified, the Bank may reconsider the performance of the requested task. The report submitted via Customer Service must be confirmed in writing within three Business Days at the latest. The Client bears full liability for damages arising from the incorrect usage of IB.

3. Following this report, the Bank is authorised to disable the use of IB. The Client undertakes to cooperate effectively with the Bank during the implementation of corrective measures proposed by the Bank.
4. The Client is authorised to ask the Bank for written confirmation that the loss/theft/abuse of Security Elements was reported to the Bank; however, the Client may do so maximally within 18 months of reporting according to paragraph 1 of this Chapter of the Conditions.
5. The Client agrees that the Bank reserves the right to block the use of IB especially in the following cases:
 - if necessary for serious, in particular, security reasons,
 - suspicion or attempted abuse of IB,
 - failure to fulfil the contractual conditions between the Bank and Client, in particular the Agreement on IB and/or the Conditions and/or the GBC by the Client and/or User,
 - repeated flaws in operation caused by technical faults in the equipment on the part of the Client,
 - in the cases foreseen by valid legal regulations.
6. The Bank shall inform the Client immediately via telephone or in writing of IB blocking, with the exception of cases when this is contrary to legal regulations.
7. If the Client ascertains that access to IB has been blocked, the Client is obliged to undertake without undue delay all the steps required to unblock or reacquire the access, in order to have access to information about the Payment Services provided to the Client by the Bank in accordance with the Payments Act.

X. LIABILITY

1. The responsibilities of the Client and Bank are governed by the GBC, these Conditions and by the Agreement on IB.
2. Furthermore, the Bank is not liable:
 - for cases when IB cannot be used for reasons beyond control of the Bank or its partners (interruption of power supply, interruption of connection with the Bank via the public internet, strikes, etc.) including the damage caused by such a cases, or

- for the damage incurred by the Client as a result of the violation of Client's obligations stipulated in these Conditions, or
- for the damage incurred as a result of incorrect Authorisation, non-fulfilment of the Payment Order for reasons on the part of the Client, or for reasons on the part of the payment Beneficiary.

3. The electronic communications network (public telephone lines, mobile network lines, e-mail and fax) which serve for communication between the Bank and the Client according to these Conditions are not under direct control of the Bank, and the Bank is not liable for damages incurred by the Client through their potential abuse. The protection of these networks and the confidentiality of messages sent throughout them must be ensured by the providers of the respective electronic communications services, particularly by course of Act no. 127/2005 Coll., on Electronic Communications, as amended.
4. The Bank is liable for the functionality of IB assuming fulfilment of the Agreement on IB, the Security Principles, User Guide and potential other instructions from the Bank.
5. If a malfunction of IB for reasons on the part of the Bank is found outside of the Bank's Business Hours, the Bank shall start working on its elimination on the following Business Day immediately after the start of the Bank's Business Hours.
6. All information about the IB system and services provided via IB and their use are of a confidential character, and the Client must not use this information contrary to the purpose for which it was provided to the Client.
7. The Client is liable for incorrectly entered data and technical flaws on the part of the Client.
8. The Client is liable to the Bank for damages incurred by the Bank in consequence of the violation of its obligations according to the Agreement on IB, these Conditions and the GBC, if applicable.

XI. EXPIRY OF THE CONTRACTUAL RELATION

1. The Bank is authorised to terminate the Agreement on IB in the way provided by the Agreement on IB and the GBC even in the event of expiry of the Agreement on CA, from which the Bank is authorised to deduct payments for the provision of IB (the so-called basic CA).
2. The Agreement on IB also expires on the date of termination of the Agreement on Client's last IB connected CA.
3. The Bank's right to withdraw from the Agreement on IB according to the GBC is not affected.
4. In the event of termination of the Agreement on IB, access to the Client's account via IB will be automatically cancelled even for all of its Users.

FINAL PROVISIONS

1. These Conditions come into force and effect on January 2011.