TERMS AND CONDITIONS OF IPKO BIZNES ELECTRONIC BANKING SERVICES

Bank Polski

Valid from 14.09.2019

§ 1 General provisions

These Terms and Conditions of iPKO biznes Electronic Banking Services („**Terms**") define the principles of providing iPKO biznes Electronic Banking services to corporate customers of PKO Bank Polski SA Niederlassung Deutschland.

§ 2 Definitions

The terms used herein shall have the following meanings:

1) Administrator – a User acting on behalf of the Account Holder that manages User authorisations granted by the Account Holder, or, in the case of entrusting the Bank with the task of parametrisation of User authorisations indicated by the Account Holder, the Administrator is the User indicated by the Account Holder that has the possibility to view the administration section of the iPKO biznes Context,

2) Access Activation – providing access to iPKO biznes electronic banking, based on a request from the Account Holder,

3) Authorisation – giving the Bank consent by the Account Holder or the User to execute a Payment Order and an Order, as well as other actions performed by means of electronic access channels, preceded by User authentication or strong User authentication,

4) Electronic Access Channel – technical solutions provided to the User by the Bank that enable using the services by means of wired and wireless connectivity and communication devices, in particular the following channels:

a) on-line,

b) telephone,

c) mobile,

(the particular access channels can differ in terms of the scope of offered options and functions, and the current, detailed description of functions provided through them is available in the information materials on the website),

5) Password – access password; individual authentication data in the form of an alphanumeric sequence of characters used to verify the User in iPKO biznes electronic banking,

6) User Identifier – individual authentication data in the form of a unique number assigned to the User, used to identify the User during logging onto the iPKO biznes electronic banking service,

7) Individual Authentication Data – individual data provided by the Bank for the purposes of authentication, which may be used also for the expression of consent in relation to a placed Order, including for the purposes of Authorisation,

8) Payment Instrument – individualised device or set of procedures used by the Account Holder to place a Payment Order,

9) Single-use Code – individual authentication data, in the form of a numeric sequence of characters, used for the Authorisation of an Order; single-use codes are provided in the form of a single-use code card in the form of a chip card or a code card in the form of a chip card with a digital public key certificate, or are generated by the iPKO biznes mobile token or by the Vasco DigiPass 270 token,

10) Context – set of accounts and list of Users authorised to use those accounts in iPKO biznes electronic banking,

11) Notification – information communicated to the Account Holder by means of electronic banking offered by the Bank, Corporate Customer Service Centre or placed in Branches or on the websites of the Bank, or in bank statements,

12) Strong Authentication – authentication that ensures the protection of data confidentiality, which uses at least two elements from the categories: knowledge, possession, and User inherence,

13) Vasco DigiPass 270 Token – a cryptographic device that generates single-use codes used for the verification of the User identity and for the Authorisation of Orders while using iPKO biznes electronic banking,

14) Agreement – the respective Account Agreement,

15) Service of confirming that the amount necessary to make a payment transaction is available in the account – on-line service consisting in providing information on the funds available in one or more accounts held by the Account Holder with either another payment service provider or with more than one payment service providers,

16) Service of access to account information – on-line service consisting in providing consolidated information on at least one account held by the Account Holder with either another payment service provider or with more than one payment service providers,

17) Payment initiation service – service consisting in initiating a Payment Order by the provider providing the payment transaction initiation service at the request of the Account Holder from the account held with another payment service provider,

18) Authentication – verification of the User identity or the validity of the payment instrument used by the Bank, performed with the use of individual authentication data,

19) User – a natural person having full legal capacity or the capacity to perform other actions within the scope of the authorisations granted to them, authorised by the Account Holder to use iPKO biznes electronic banking and acting on behalf of and for the benefit of the Account Holder.

§ 3 Access and using electronic banking

1. Having appropriate hardware and software, necessary for cooperation with the Bank, is the prerequisite for using access to electronic banking. The Bank shall not guarantee or assume liability with respect to software and devices offered by third parties as regards the possibility to apply and use these for the purposes of User Authentication.

2. Requirements with regard to the hardware and software are communicated by the Bank to the Account Holder on the Bank's website.

3. The Bank shall inform the Account Holder about the principles of correct and safe use of electronic banking and about potential fraudulent transactions, about the occurrence of suspicious incidents and untypical attacks.

4. The information referred to in sections 1-3 is communicated by the Bank to the Account Holder on the Bank's websites or in Notifications, or via the telephone service.

5. Information communicated through a different channel (such as e-mail) concerning correct and safe use of electronic banking shall not be reliable information.

6. Banking products and services resulting from the scope of services provided by the Bank may be made available in electronic banking. The Account Holder using iPKO biznes electronic banking has also the possibility to conclude agreements through electronic access channels, provided that such method of concluding them has been made available by the Bank.

7. Information regarding banking products and the scope of services provided by the Bank as part of electronic banking, as well as the rules and method of using electronic banking, including in particular the settings and functionalities of the service, is available in the informational materials on the Bank's website.

8. The Account Holder shall be obliged to familiarise themselves with the information referred to in sections 6-7 before starting to use electronic banking.

9. A change to any information, rules or method of using electronic banking, which are referred to in sections 6-7, in particular the settings and functionalities of the service, as well as a change of the version of electronic banking, shall not require the consent of the Account Holder.

10. The User is obliged to log on to and place Orders in electronic access channels only in person, using individual authentication data, and to:

1) keep secret the information ensuring secure use of electronic banking and not to communicate or disclose individual authentication data to third parties, including the Password, single-use codes or information provided to the Bank for verification purposes. This does not apply to the use of the payment initiation and account information service, in accordance with § 4.

2) properly secure the hardware and software, through which electronic banking is used, in particular by using:

a) exclusively legal software, its ongoing updating and installation of system patches, in accordance with the manufacturers' recommendations,

b) up-to-date anti-virus and anti-spam software, and firewall,

c) the most recent versions of web browsers,

d) passwords securing access to the computer, in particular if a device is used by more than one person,

e) other solutions recommended by the Bank, provided on the Bank's website,

3) immediately report a loss or destruction of individual authentication data or the detection of unauthorised, non-executed or improperly executed Orders, in the case of obtaining the information referred to in section 5 or in the case of suspecting unauthorized or illegal use of individual authentication data

- by telephone, to the number provided in the informational materials regarding electronic banking,
- in person at a Branch of the Bank.

4) immediately report to the competent law enforcement authorities a loss or destruction of individual authentication credentials or software, used for the purpose of using electronic banking.

5) with regard to using individual authentication data, the User is in particular obliged to:

a) keep secret the authentication data that require knowledge of something that only the User knows, including not making these credentials available verbally (e.g. by telephone) or in text form (e.g. by e-mail or messaging apps used in smartphones), not saving them in electronic form unprotected (e.g. saving them in plain text on a computer or a mobile device) and not placing or saving these data on devices for identification of the User, which data use something that only the User has or characteristics inherent to the User,

b) in the case of using individual authentication data that use something that only the User has:
   - not provide these credentials to third parties,
   - prevent third parties' access to mobile terminal equipment (e.g. mobile phone) or the electronic banking applications installed on such equipment,
   - remove from the mobile terminal equipment the applications used for electronic banking before handing this phone to third parties (e.g. through sale),
   - not share, outside electronic banking, such data as e.g. single-use codes verbally (e.g. by telephone) or in text form (e.g. through e-mail or messaging apps used on smartphones),
   - protect the access data obtained from the Bank, which enable the use of such authentication data, from third-party access.

c) in the case of using individual authentication data that use characteristics inherent to the User – to ensure that such elements owned by other persons are not saved on mobile terminal equipment used for electronic banking. If, however, such equipment already contains such elements owned by third parties, such elements of individual authentication data shall be used that require the knowledge of something that only the User knows (e.g. Password),

6) The telephone number used for receiving the single-use codes shall be removed or changed if it is no longer used by the User for the purpose of using electronic banking,

7) Before executing the Order received from the User, the Bank shall inform the User of the obtained data, such as the amount, the account number of the payee via the agreed device used for electronic banking (e.g. mobile terminal equipment). The User is obliged to verity these data before Authentication, and should the data received from the Bank differ from the data sent by the User beforehand, to cancel the Order execution and immediately notify the Bank thereof.

11. In order to ensure security of Orders placed by the User, the Bank shall apply Authorisation of Orders placed in electronic banking with the use of individual authentication data. The Bank reserves the right to refuse to execute orders placed through the on-line or telephone service, when the circumstances justify doubts as to the identity of the User or their authenticity. If the User attempts to obtain access to highly sensitive data concerning payment within the meaning of § 1(26) sentence 1 of ZAG (e.g. change of the Account Holder's address), the User must use additional authentication data if the User has previously accessed the account using only one authentication method, where the name and surname of the account holder and the account number shall not be considered highly sensitive data concerning the payment

12. The Banks records conversations conducted through the telephone service and keeps record of the Orders placed through electronic access channels. The recorded User's Orders constitute a proof of placing a given order.

13. The User is entitled to access information constituting bank secrecy to the extent resulting from the granted authorisations.

14. All Orders placed in the electronic form by a person who has been correctly verified as the User are treated as orders of the User, acting on behalf of the Account Holder. The Bank shall not be liable for execution of orders made in violation of the rules laid down in section 10.

15. The Bank may establish temporary limits, expressed in amounts, on payment transactions that can be ordered through specific electronic access channels.

16. Information in this regard shall be provided on the Bank's website.

17. The Bank reserves the right to block access to electronic banking fully or partially, including blocking particular individual authentication data, for justified reasons related to security of access to those services or in connection with a suspicion of unauthorised use of access to electronic banking or wilful placement of unauthorised payment order with the use of access to electronic banking or when the Bank has the right to terminate the Agreement for cause.

18. The Bank, by means of electronic access channels, shall inform the Account Holder about blocking access to electronic banking, including blocking particular individual authentication data, before blocking, or, should this be impossible, immediately after performing that action, unless transmission of that information is unjustified for security reasons or is prohibited under the law.

19. The blockade shall remain effective, and individual authentication data will be replaced, when the reason for which it was imposed ceases to exist. The User shall be immediately informed of removal of the blockade.

20. The Account Holder shall obtain the possibility to use iPKO biznes electronic banking after:

a) familiarising themselves with the informational materials regarding electronic banking,

b) concluding an Agreement, annex or appendix to the Agreement,

c) determining the authorisations, including appointment of at least one User to act as Administrator,

d) receiving individual authentication data,

e) activation of access.

21. Having the following individual authentication data shall be the prerequisite for using iPKO biznes electronic banking:

a) Password,

b) User identifier,

c) single-use code card in the form of a chip card with a reader or the application of iPKO biznes mobile token or Vasco DigiPass 270 token.

22. The User's functional authorisations to use electronic banking shall be established by the Administrator appointed by the Account Holder, using of the administrative functions of the system, or by the Bank, on the basis of an Order from the Account Holder in the form of a separate request for configuration of access to iPKO biznes.

23. The Bank shall not be liable for the effects of the actions of the Administrator managing the Users' authorisations on behalf of the Account Holder and the Users. In the event of entrusting the Bank with the task of parametrisation of User authorisations indicated by the Account Holder, the Bank shall not be liable for effects of such performance according to the Account Holder's instructions.

24. The Bank shall not interfere with the justifiability of the models of authorisations, including patterns of acceptance of Payment Orders created by the Administrator managing the User authorisations on behalf of the Account Holder.

25. Payment Orders are executed according to the Specific Terms and Conditions applicable with respect to a given type of order (e.g. Terms and Conditions for the execution of transfer orders).

§ 4 Use of the payment initiation and account information service

1. The User may, pursuant to § 675f(3) of BGB (German Civil Code), place payment orders or obtain account information through a payment initiation service provider in accordance with § 1(33) of ZAG or account information service provider in accordance with § 1(34) of ZAG, who will establish a technical connection with the Bank for this purpose.
2. The Bank is entitled to deny access to the account with respect to payment initiation service providers or account information service providers if there are objective and demonstrable grounds for that, in connection with an unauthorised or illegal access of such a service provider to the account. The Bank shall inform the Account Holder of access denial accordingly. Providing such information shall be performed, as far as possible, before access denial, and directly after access denial at the latest. The Bank may refuse to provide the reasons for access denial if the Bank would violate the law by doing so. The Bank will restore access when the reasons for access denial cease to exist and will immediately inform the Account Holder thereof.

§ 5 Liability

1. The Bank's liability for executing an unauthorised payment order or for a non-executed, incorrectly executed or late executed order shall be governed by the Specific Terms and Conditions applicable for the respective order type.

2. Any claims and objections raised by the Account Holder against the Bank as a result of non-execution or incorrect execution of a payment order, or as a result of executing an unauthorised payment order, shall be excluded if the Account Holder fails to duly notify the Bank thereof within a period of 13 months of being debited for an unauthorised or incorrectly executed payment order at the latest. This period shall start to run only once the Bank has informed the Account Holder about the debit entry for the payment orders through the agreed account information channel no later than one month after the debit entry was made; otherwise, the date on which the Account Holder is informed shall determine when the period starts to run.

3. If the unauthorised payment orders are executed before requesting access blocking as a result of using misplaced, stolen, or otherwise lost

individual authentication data or using them in another fraudulent manner, the Account Holder shall be liable, up to a maximum of EUR 50.00, for any losses caused by the above, regardless of any fault on the User's part.

4. The Account Holder shall not be liable in accordance with section 1 above if:

– the Account Holder was unable to notice the loss, theft, misplacement of the individual authentication data or using them for fraudulent purposes prior to executing the unauthorised transaction, or
– the loss of the individual authentication data was caused by an employee, agent, branch of the Bank or another entity acting on behalf of the Bank.

5. If the Account Holder is not a consumer, the Account Holder shall suffer the loss incurred due to unauthorized transactions even above the maximum amount of EUR 50.00 if the User has negligently breached the obligations imposed on the User under these Terms. If the Bank has contributed to the loss through a breach of its obligations, the Bank shall be liable for the incurred losses according to the principles of contributory negligence, for the part for which it is liable.

6. The Account Holder is not obliged to cover the loss referred to in sections 3, 5, 7 if the Account Holder was unable to report the request for access blocking because the Bank failed to provide the option of accepting such a report. The same shall apply to a situation where the Bank has failed to request Strong Authentication pursuant to § 1(24) of ZAG.

7. In cases where unauthorised transactions have been made prior to the request for access blocking and the User has acted with fraudulent intent or has intentionally or as a result of gross negligence breached their obligation to exercise due diligence, referred to herein, the Account Holder shall be fully liable in respect of any losses incurred as a consequence thereof. In particular, breach of § 3(10) shall be deemed gross negligence on the part of the User.

8. The liability for a loss arising in the period in which the transaction limit applies shall be limited in each case to the applicable transaction limit.

9. Sections 4, 6, 8 shall not apply if the User has acted with fraudulent intent.

10. Following the receipt of access blocking request, The Bank shall be liable for losses arising due to unauthorised Payment Orders executed by means of electronic banking. This provision shall not apply, however, if the User has acted with fraudulent intent.

§ 6 Final Provisions

1. Unless otherwise agreed in the Terms, the cooperation under the Terms shall be governed by the General Terms and Conditions ("GTC") between the customer and PKO Bank Polski SA Niederlassung Deutschland. In addition, specific scope of cooperation shall be governed by Specific Terms and Conditions containing exemptions from GTC or supplements thereto. Specific Terms and Conditions shall in particular apply to credit transfers and direct debit payments. The content of the aforementioned terms and conditions is available at the Bank. The participants may also request to have the copy of the GTC or Specific Terms and Conditions delivered at a later date.

2. These Terms may be amended pursuant to Clause 1(2) of the GTC.