TERMS AND CONDITIONS APPLYING TO THE ELECTRONIC SIGNATURE

The below Terms and Conditions Applying to the Electronic Signature (hereinafter the "**Conditions**") represent Product conditions in terms of the General Terms and Conditions of the Bank (hereinafter the "**General Conditions**"). The Conditions form part of the Contract and the Certificate Holder is obliged to familiarise himself/herself with them and to comply with them.

Capitalised terms used herein shall have the meaning as defined in Article 7 hereof.

Article 1. Electronic Signature Creation Methods

1.1 The Certificate Holder may use his/her Electronic Signature based on the method described as "the certificate stored on a chip card (smart card)" when utilizing selected Banking Services, in particular direct banking services. The aforementioned method may be used both for the authentication of the Certificate Holder and for the Electronic Signature as such.

1.2 Only the Certificate Holder shall be entitled to use the Electronic Signature creation method provided under the Contract.

1.3 The Bank shall be entitled to charge to the Certificate Holder a fee as per the Tariff of Fees for the provision and use of the method and related services.

1.4 The Contract shall be governed by the law of the Slovak Republic, in particular by the Commercial Code[1].

1.5 By signing the Contract, the Certificate Holder confirm that he/she has familiarised himself/herself with the contents and meaning of the Certification Policy and the Decalogue of the Security, and he/she shall abide by their provisions and adhere to the principles contained therein.

1.6 Technical information concerning the Certificate is available in the Technical Terms and Conditions.

Article 2. Certificates

2.1 The Bank may only issue the Certificate in the form of a Certificate stored on a chip card (smart card).

Certificate Stored on a Chip Card (Smart Card)

2.2 **Activation**. Upon entering into the Contract and in cooperation with the Certificate Holder, the Bank shall send the Certificate Holder a one-time password to the agreed GSM mobile telephone number so that he/she can create the Certificate at MůjProfil portal, or the Bank shall create the Certificate, including the generation a Private and Public Keys, and store it on a chip card (smart card). The one-time password shall remain effective for a period of 3 days from being sent. At the same time, the Bank shall deliver to the Certificate Holder the chip card and an envelope containing the PIN and PUK Codes.

The mobile telephone number indicated by the Certificate Holder in the Contract as that to which the SMS messages should be delivered must be identical to that specified by the Client in the Authorisation Order with respect to the specific Certificate Holder and must not be used for the same purpose by another Certificate Holder as long as the given Certificate is valid. The Bank shall not be held liable for any damage caused by the fact that the Certificate Holder might have stated a wrong mobile telephone number to which the Bank should deliver the SMS messages.

Article 3. Validity of the Certificate

3.1 **Validity of the Certificate.** The Certificate shall be valid for 2 years, unless the Conclusive Date occurs or the Contract is terminated in the meantime. The term of validity of a specific Certificate is specified in the Certificate itself or can be determined at MůjProfil portal. The Certificate Holder may use a valid and effective Certificate while utilising the Services. The Certificate Holder also may ask for the renewal of the Certificate via MůjProfil portal before its expiry

1 Act No. 5131991 Coll. – the Commercial Code, as amended.

3.2 If the Certificate Holder asks for the renewal of the Certificate before its expiry, the Bank shall issue him/her with a new Certificate under the existing Contract, unless the Conclusive Date occurs or the Contract is terminated before the date of the submission by the Certificate Holder of the request for the renewal of the Certificate. The Bank shall issue the new Certificate in the same form and with the same identification data as the previous one. As of the moment of issue of the new Certificate, the Certificate Holder shall not be allowed to use the previous one any longer. The procedure described in Article 2 hereof shall accordingly apply to the issue of a new Certificate.

3.3 If the identification data of the Certificate Holder stated in the Contract (including the mobile telephone number to which the SMS Messages are to be sent) should change, the Certificate Holder shall be obliged to notify the bank of this fact without any unnecessary delay in writing and to execute an amendment to the Contract with the Bank, or to apply for the issue of a new Certificate. If the electronic address of the Certificate Holder stated in the Contract should change, the Certificate Holder shall be obliged to notify the Bank in writing at the Client's Point of Sale. The Bank shall not be obliged to accept any change to the mobile telephone number to which the SMS Messages are to be sent or to the agreed-upon electronic address, if the new number/address are not identical to those specified by the Client in the Authorisation Order with respect to the specific Certificate Holder whose identification data should be changed.

Article 4. Blocking the Certificate

4.1 If the Certificate is blocked, its validity shall be suspended until the Certificate Holder asks the Bank to reactivate it. The Certificate Holder shall be informed about the method blocking on the contact telephone number specified in the Contract.

4.2 **Blocking by the Certificate Holder**. The Certificate Holder may request the method blocking at any time on the telephone number +420 955 551 552, at any of the Bank's points of sale or at MůjProfil portal on the Bank's website. The Certificate Holder shall be obliged to request the method blocking any time he/she suspects that the method might have been misused.

4.3 **Blocking by the Bank.** The Bank shall block the Certificate and possibly also demand that the Certificate Holder apply for the reactivation of the Certificate if at least one of the following events occurs:

- The method has been arranged on the basis of false, incomplete or misleading information,
- The identification data that form part of the method is no longer valid,
- The Certificate Holder is in breach of any of his/her duties under the Contract,
- The mobile telephone number to which the Bank should send the one-time password and SMS Messages has been used in several Contracts and/or for several Clients,
- The Bank ceases to provide the given method,
- The Bank is required to do so by law,
- Security risks have increased or might increase, or measures relating to the erroneous inputting of security data or the use of the method have become stricter.

4.4 For Certificates stored on a chip card (smart card), the chip card shall be blocked after the third incorrect PIN entry. The Certificate Holder may ask for the chip card to be unblocked at the Client's Point of Sale or can do it by himself/herself using the KB Cryptoplus application. In both cases, the Certificate Holder must enter the PUK Code to unblock the chip card.

Article 5. Security

5.1 **Security Prior to Activating the Method – loss or theft**. If the mobile telephone to which the one-time password should be sent is lost or stolen or the e-mail address to which the one-time password should be sent is misused or blocked before you create the Certificate, or the mobile telephone to which the one-time password should be sent is lost or stolen prior to activating the method, the Certificate Holder shall be obliged to notify the Bank without any unnecessary delay to the telephone number **+420 955 551 552** and agree upon an alternative method of the delivery of a new one-time password. The Bank shall subsequently invalidate the old password. The Bank can deliver the one-time password at the electronic address of the Certificate Holder, if such an address is stated in the Contract, in the case of the Certificate.

5.2 **Certificate.** The Certificate Holder shall be fully responsible for the process of the creation of the Certificate, including the generation of a Public and Private Key on the PC that the Certificate Holder has used for this purpose. Being the sole user of the Certificate including the Private Key, the Certificate Holder shall be liable for their use.

5.3 A Private Key stored in a data file is protected by a password. A Private Key stored on a chip card is

protected by a PIN Code.

5.4 The Certificate Holder shall be obliged to protect his/her Private Key, the password and, as the case may be, the PIN and PUK Codes, to be used with the Private Key throughout the entire term of the validity of the Certificate, in particular from a possible loss, disclosure to a third party, alteration, or unauthorised use. The password or the PIN and PUK Codes to be used with the Private Key must not be stored in the same place or on the same media as the Private Key and may never be stored in any manner that would make them accessible to third parties. In particular, the Certificate Holder must not leave an unsecured Private Key in the PC with a password entered and the key activated, or leave the chip card inserted in the chip card reader outside the time when he/she is logging into a given Banking Service or is using the Electronic Signature. The Certificate Holder must continuously make sure that the Certificate has not been lost, stolen, misused or used without authorisation.

5.5 **Loss of the chip card (smart card).** If the chip card (smart card) on which the personal certificate is stored is lost, or if the chip card security features are lost, the Certificate Holder shall be obliged to notify the Bank without any unnecessary delay to the above telephone number and apply for blocking the personal certificate.

5.6 The Bank shall be entitled to suspend the Service temporarily for serious reasons, particularly those of a security nature. In cases as stipulated in the Act on Bankruptcy and Restructuring,[2] the Bank shall be entitled to block access to the Service or suspend the provision of the Service.

5.7 The Certificate Holder shall be obliged to notify the Bank without any unnecessary delay of the loss, theft or any ascertained risk of threatened misuse of the Certificate (the password, PIN and PUK Codes) and request the blocking of the specific method.

General Provisions

5.8 The Certificate Holder shall discharge his/her duty to inform the Bank pursuant to these Conditions at the Client's Point of Sale, by e-mail delivered at the address indicated in the relevant Product Terms and Conditions, or over the telephone to the above telephone number. If the Certificate Holder fails to fulfil the duty to inform the Bank within 3 Business Days from the day on which such duty has arisen without being prevented from doing so by particularly serious reasons, the Certificate Holder shall be deemed to have failed to notify without any unnecessary delay.

5.9 Electronic communications networks (public telephone lines, mobile network lines, e-mail and fax) used for mutual communication between the Bank and the Certificate Holder pursuant to these Conditions are beyond the direct control of the Bank; therefore the Bank is not liable for any damage caused to the Certificate Holder by their potential misuse. The Certificate Holder acknowledges that the relevant providers of electronic communications services are obliged to secure the protection of these networks and the confidentiality of messages sent via the networks, as envisaged particularly in Act No. 610/2003 Coll., on Electronic Communications, as amended.

5.10 The Bank shall not be held liable for any unauthorised or erroneously performed payment transactions, for any damage incurred by the Certificate Holder as a result of a breach of his/her duties set forth herein, or for any loss or damage resulting from an incorrect authorisation or non-execution of an Order due to reasons caused by the Certificate Holder or a payee. The bank shall neither be held liable for any misuse of the Certificate resulting from misuse of a PC used by the Certificate Holder (e.g. caused by software supplied by another supplier, a virus infected PC, hardware fault etc.).

5.11 The Bank shall not be held liable for cases where the Certificate cannot be used due to circumstances that are beyond the Bank's control and/or beyond the control of the Bank's partners (in particular a power failure, interruption to the connection with the Bank via a public telephone/Internet network, strike, etc.). The Bank shall not be obliged to demonstrate to the Certificate Holder that it has followed the procedure that makes it possible to verify that an Order has been submitted, a particular payment transaction has been authorised, correctly documented and entered in the books, and it has not been affected by technical problems or other flaws.

5.12 The Bank shall hold the Certificate Holder liable for any damage it may suffer in case the Certificate Holder breaches his/her duties set forth herein.

Article 6. Termination of the Contractual Relationship

6.1 The Contract shall expire/be terminated:

a) By a notice of termination served by either of the contracting parties. Both the Bank and the Certificate

2 Act No. 7/2005 Coll. on Bankruptcy and Restructuring, as amended.

Holder shall be entitled to terminate the Contract in writing at any time without giving a reason. The notice of termination served to the Bank shall become effective on the next succeeding Business Day following the day of receipt of the notice. The notice of termination served to the Certificate Holder shall become effective on the last day of the month following the month in which he/she receives the notice.

b) As at the Conclusive Date.

c) The Initial Contract for the Issue and Use of a Personal Certificate shall expire automatically upon the expiry of the Certificate.

6.2 The Bank's right to cancel the Contract in accordance with the General Conditions shall not be prejudiced by this provision.

6.3 The Certificate Holder shall not be allowed to use the Certificate after the expiry/termination of the Contract.

Article 7. Definition of Terms

7.1 Capitalised terms used herein shall have the following meaning:

"**Administration Order**" shall mean a power of attorney by which the Client authorises the Certificate Holder to use a particular DB Service to the extent set forth in the Administration Order.

"**Bank**" shall be Komerční banka, a.s., registered office at Praha 1, Na Příkopě 33/969, Postal Code: 114 07, Czech Republic, IČO (Company ID): 45317054, entered into the Commercial Register kept by the Municipal Court in Prague, Section B, Insert 1360, acting through its organisational unit Komerční banka, a.s., pobočka zahraničnej banky (a foreign bank branch), registered office at Hodžovo námestie 1A, Postal Code: 811 06, Bratislava, IČO (Company ID): 47 231 564, Slovak Republic, entered into the Commercial Register kept by the District Court in Bratislava I., Section: Po, Insert No. 1914/B.

"**Banking Services**" shall mean any banking deals, services and products the Bank is entitled to deliver pursuant to applicable law.

"**Business Day**" shall mean a day that does not fall on a Saturday, a Sunday, a public holiday or other holidays within the meaning of the applicable law, on which the Bank is open for the provision of Banking Services and on which other institutions that take part in the provision of Banking Services, or on which the provision of the Banking Services depends, are open and provide the relevant services. A day declared as a non-business day by the Bank due to particularly serious operational reasons shall not be considered a Business Day.

"**Certificate**" shall mean an Electronic Signature creation method consisting in creating a personal certificate that makes it possible to authenticate a signatory. It contains the Public Key, Private Key and Certificate Holder's identification data.

"**Certificate Holder**" shall mean a person who has entered into the Contract with the Bank and who, while entering and discharging the Contract, acts under an employment relationship existing between him/her and the Client as at the date of execution of the Contract, or while performing mutually agreed activities for any of the Clients pursuant to a mutual agreement, either as a Plenipotentiary or as a Statutory Body.

"**Certification Policy**" shall mean a document in which the Bank sets forth the rules and procedures for using the Certificate and its specification, which the Bank is entitled to modify. The Bank publishes the Certification Policy on its website. The Certification Policy is also available at the Client's Point of Sale. This document is not a Notice as envisaged by the General Conditions.

"**Chip Card PIN**" shall mean a four-digit personal identification number used to verify the holder's authorisation to handle the chip card.

"**Client**" shall mean a person who has entered into the contract for the provision of a given Banking Service with the Bank and on whose behalf the Certificate Holder is entitled to act as a Plenipotentiary or a Statutory Body, within the scope and to the extent of the Administration Order, when the Banking Service is provided.

"**Client's Point of Sale**" shall mean the Bank's point of sale located at the Bank's registered address or another branch/point of sale, if it exists.

"Conclusive Day" shall be (i) a day on which the Bank learns, in a trustworthy manner, about the death of a Certificate Holder, i.e., a day on which conclusive documents attesting the fact that the Certificate Holder died or was declared dead are delivered to the Client's Point of Sale (these documents can be, e.g., a death certificate, a court or notary memorandum of performing the inheritance proceedings, decision of the court with a legal power clause concerning the declaration of the Certificate Holder's death, or (ii) a day not earlier than the date as of which all authorisations and access rights of the Certificate Holder as a Plenipotentiary or Statutory Body within the meaning of the Administration Order issued by a given Client shall have been cancelled, provided that all authorisations and access rights of the Certificate Holder as a Plenipotentiary or Statutory Body with respect to any Client shall have ceased to exist.

"**Contract**" shall mean a contract in which the Bank undertakes to issue the Certificate Holder with the Certificate as an Electronic Signature creation method.

"D**B Service**" is the *Profibanka* direct Banking Service the Client uses under the Contract for the Provision and Use of Direct Banking.

"**Decalogue of the Safe Internet Banking**" is a document in which basic principles of safe use of the Internet banking are defined, which the Bank is entitled to amend. The Bank has made The Decalogue of the Safe Internet Banking public on its website. It is also available at the Bank's points of sale. This document is not a Notice as envisaged in the General Conditions.

"**Electronic Signature**" shall mean an advanced electronic signature within the meaning of the Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, based on the methods the Bank makes available under the Contract.

"**General Conditions**" shall mean the General Business Terms and Conditions issued by the Bank.

"**Initial Contract for the Issue and Use of a Personal Certificate**" shall mean the contract under which the Bank undertakes to issue the Client with the Personal Certificate entered into pursuant to the Terms and Conditions of the Issue and Use of a Personal Certificate.

"**MůjProfil**" shall mean a portal for the support and management of the Electronic Signature creation methods. Můj Profil is accessible to the Certificate Holder on the Bank's website, to which the Client may log in using any Electronic Signature creation method or directly from the DB Service.

"**Notices**" shall mean communications in which further conditions and technical features of providing the Banking Services are specified in accordance with the General Terms and Conditions or relevant Product conditions. The following documents, without limitation to them, are not Notices: The following documents, without limitation to them, are not Notices: the Certification Policy and the Decalogue of the Security.

"**Payment Services**" shall mean Banking Services falling within the scope of payment services as envisaged by the Payments Act (e.g., money transfers, issuing of payment instruments and cash deposits/withdrawals).

"**Plenipotentiary**" shall be a natural person other than a Statutory Body, who is the Certificate holder entitled to use the DB Service to the extent set forth in the Administration Order.

"**Private Key**" shall mean the data used for creating the Certificate Holder's electronic signature in the form of a Certificate.

"**Product Terms and Conditions**" shall mean the Bank's terms and conditions regulating the provision of separate Banking Services.

"**Public Key**" shall mean the data used for verifying the Certificate Holder's electronic signature in the form of a Certificate.

"**PUK Code**" shall mean an eight-digit code used to unblock the chip card.

"**Service**" shall mean any Banking Service provided to the Client and utilizing the Certificate.

"**Statutory Body**" shall mean, notwithstanding the manner in which they act externally on behalf of the Client – legal person; a natural person – statutory body of the legal person; a member of a statutory body of the legal person; or another natural person in a position similar to that of a statutory body of a legal person authorised by the Client by an Administration Order to use the DB Service.

"**Tariff of Fees**" shall mean a list of all charges, other fees and payments for the Banking Services and operations associated with the Banking Services.

"**Technical Terms and Conditions**" shall mean a document in which the Bank sets technical terms of the provision of the direct banking services, which the Bank is entitled to amend. The Bank has made the Technical Terms and Conditions public on its Internet pages. The Technical Terms and Conditions are not a Notice as envisaged in the General Conditions.

7.2 Any reference to the Bank's website shall mean a reference to www.kb.sk or other web addresses the Bank currently uses or shall use while providing the Banking Services.

Article 8. Final Provisions

8.1 Wherever the contracts and other documents entered into by and between the Bank and the Client, or the contractual documents that are part of such contracts, refer to the Terms and Conditions of the Issue and Use of a Personal Certificate, this shall mean the Terms and Conditions Applying to the Electronic Signature.

8.2 The Bank is entitled to amend these Conditions from time to time in the manner set forth in the General Conditions.

8.3 These Conditions come into effect as of 10 February 2022. At the same time, these Conditions repeal and replace the Terms and Conditions of the Issue and Use of a Personal Certificate issued by the Bank and connected to the Contract for the Issue and Use of a Personal Certificate effective as from 19 May 2019.