TERMS AND CONDITIONS APPLYING TO CERTIFICATES

This English version of the contractual document is for information only and is not legally valid. In the event of any discrepancies between the Czech and English versions, the Czech version shall prevail.

These terms and conditions describe in detail the rights and duties arising from the contract for a personal or business certificate. Please read this document thoroughly. We shall gladly answer any of your questions.

Article 1. Terms of Use Certificate

1.1 The Personal Certificate may only be used by you. The Company Certificate may also be used by a natural person whom you have authorised and to whom you have handed over the Company Certificate.

1.2 You shall pay a fee per the Tariff of Fees for the issue of a Certificate and related services.

1.3 The Contract under which we shall issue the Certificate shall be governed by the law of the Czech Republic, in particular by the Civil Code[1] starting from its effective date, even in case of Contracts entered into before that date. However, the execution of the Contract, as well as any and all rights and duties arising under the Contract before the effective date of the Civil Code, shall be judged based on previous law.

1.4 By signing the Contract, you confirm that you have familiarised yourself with the contents and meaning of the Certification Policy and the Decalogue of the Security, and you shall abide by their provisions and adhere to the principles contained therein. If we issued to you the Company Certificate, you shall be obliged to acquaint all individuals who are entitled to use it with the aforesaid documents and see to it that they adhere to the principles contained therein.

Article 2. Issuing the Certificate

2.1 You may apply for the Personal Certificate in the form of a Personal Certificate stored either in a data file or on a chip card (smart card). You may apply for the Company Certificate only in the form of a Company Certificate stored in a data file.

Personal and Company Certificates Stored in a Data File

2.2 After entering into the Contract, we shall send to you an SMS message to the agreed GSM mobile telephone number, containing a one-time password for the creation of the Certificate, including the generation of a Private and Public Key. In case of the Company Certificate, we may send you the password by e-mail at an agreed electronic address. The one-time password shall remain effective for a period of 30 days from being sent to you. After the lapse of the aforesaid period, we may only issue a new Certificate to you upon entering into a new Contract.

2.3 The GSM mobile telephone number you indicate in the Contract as that to which we should send the one-time password and/or Authorisation SMS Messages must not be used for the same purpose by another Client. We shall not be held liable for any damage caused by the fact that you might have stated a wrong GSM mobile telephone number or electronic address to which we should deliver the one-time password and/or Authorisation SMS Messages.

2.4 You shall create the Certificate using the one-time password in the Certification Wizard. Before that, you should check the accuracy of your identification data displayed and to verify that they are consistent with those stated in the Contract.

2.5 If the GSM mobile telephone to which the one-time password sent is lost or stolen, or the e-mail address is misused or blocked before you create the Certificate, you shall be obliged to notify us without any unnecessary delay at the telephone number +420 955 551 552 and agree upon an alternative method of the delivery of a new one-time password. We shall subsequently invalidate the old password. We can deliver the one-time password at your electronic address, if it is stated in the Contract.

Personal Certificate Stored in a Data File in an Internet Browser

2.6 You may transfer the issued Personal Certificate stored in a data file to a specific Internet browser and, subsequently, use it stored in the data file *and* transferred to the Internet browser at the same time. Further information is available in the Technical Terms and Conditions.

[1] Act No. 89/2012 Coll., The Civil Code as amended.

FOR INFORMATION ONLY

Personal Certificate Stored on a Chip Card (Smart Card)

2.7 Upon entering into the Contract and in cooperation with you, we shall create the Certificate, including the generation a Private and Public Key, and store it on a chip card, or send you a one-time password at the agreed GSM mobile phone number so that you can create your Certificate in the Certification Wizard. The one-time password shall remain effective for a period of 30 days from being sent to you. At the same time, we shall deliver to you the chip card and an envelope containing the PIN and PUK.

Article 3. Validity of the Certificate

3.1 In general, the Certificate shall be valid for 2 years. The term of validity of a specific Certificate is specified in the Certificate itself or can be determined in the Certification Wizard. You may use a valid and effective Certificate while utilising the Services. You also may ask for the renewal of the Certificate in the Certification Wizard before its expiry.

3.2 If you ask for the renewal of the Certificate before its expiry, we shall issue a new Certificate under the existing Contract. The new Certificate shall be issued in the same form and with the same identification data as the previous one. As of the moment of issue of the new Certificate, you 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 your identification data stated in the Contract (including the GSM mobile telephone number to which the Authorisation SMS Messages are to be sent) should change, you shall be obliged to notify us on this fact without any unnecessary delay in writing and to execute an amendment to the Contract, or to apply for the issue of a new Certificate. If your electronic address stated in the Certificate should change, you shall be obliged to amend the address in the Certification Wizard.

3.4 Upon the expiry of the Certificate, you shall only be entitled to apply for the issue of a new Certificate after entering into a new Contract.

Article 4. Blocking the Certificate

4.1 If the Certificate is blocked, its validity shall be terminated and the Certificate may no longer be used. Information regarding the current status (validity) of the Certificate is available in the Certification Wizard. You may also consult the certificate blocking list (CBL) available at our Internet pages to check whether the Certificate has been blocked.

4.2 You may request the blocking of the Certificate at any time at the telephone number +420 955 551 552, at any of our points of sale, or in the Certification Wizard application at our Internet pages. You shall be obliged to request the blocking of the Certificate if you find any discrepancy between the content of the Certificate and the information/data in the Contract or if you suspect that the Certificate might have been misused.

4.3 We shall be entitled to block the Certificate and possibly also demand that you apply for a new Certificate if at least one of the following events occurs:

- The Certificate has been issued on the basis of false, incomplete or misleading information;
- The identification data which form part of the Certificate are no longer valid;
- You are in breach of any of your duties under the Contract;
- The GSM mobile telephone number to which the we should send the one-time password and Authorisation SMS Messages has been used in several Contracts and/or for several Clients;
- We cease to issue Certificates;
- We are required to do so by law;
- Security risks have increased or might increase, or measures relating to the use of the Certificate have become stricter.

4.4 For Certificates stored on a chip card, the chip card shall be blocked after the third incorrect PIN entry. You

FOR INFORMATION ONLY

may ask for the chip card to be unblocked at your point of sale or can do it by yourself using the KB Cryptoplus application. In both cases, the PUK code must be entered to unblock the chip card.

Article 5. Security

5.1 You shall be fully responsible for the process of the creation of the Certificate, including the generation of a Public and Private Keys, on the PC that you have used for this purpose. Being the sole user of the Certificate including the Private Key, you shall be liable for their use.

5.2 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.

5.3 You shall be obliged to protect your Private Key, the password and, as the case may be, the PIN and PUK, 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 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 a manner that would make them accessible to third parties. In particular, you 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 you are logging into a given Banking Service or are using the Signature. You must continuously make sure that the Certificate has not been lost, stolen, misused or used without authorisation.

5.4 You shall be obliged to notify us without any unnecessary delay of the loss, theft or any ascertained risk of threatened misuse of the Private Key and a related password and/or, as the case may be, the PIN and PUK, to be used with the Private Key and request the blocking of the Certificate.

5.5 You shall discharge your duty to inform us pursuant to these Conditions at your point of sale, by e-mail delivered at the address indicated in the relevant Product Terms and Conditions, or over the telephone at a number communicated to you by us. If you fail to fulfil the duty to inform us within 3 Business Days from the day on which such duty has arisen without being prevented from doing so by particularly serious reasons, you shall be deemed to have failed to notify us without any unnecessary delay.

5.6 Electronic communications networks (public telephone lines, mobile network lines, e-mail and fax) used for our mutual communication pursuant to these Conditions are beyond our direct control; therefore we are not liable for any damage caused to you by their potential misuse. 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. 127/2005 Coll., on Electronic Communications, as amended.

5.7 We shall not be held liable for any unauthorised or erroneously performed payment transactions, for any damage incurred by you as a result of a breach of your 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 yourself or a payee. We shall neither be held liable for any misuse of the Certificate resulting from misuse of a PC that you use (e.g. caused by software supplied by another supplier, a virus infected PC, hardware fault etc.).

5.8 We shall not be held liable for cases where the Certificate cannot be used due to circumstances that are beyond our control and/or beyond the control of our partners (power failure, interruption to the connection with the Bank via a public telephone/Internet network, strike, etc.). Unless you are a Qualified Client within the meaning of the General Conditions, we shall not be obliged to demonstrate that we have 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.

5.9 We shall hold you liable for any damage we may suffer in case that you breach your 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 you and we shall be entitled to terminate the Contract in writing at any time without giving a reason. If the Contract is terminated by you, the notice of termination shall become effective on the next succeeding Business Day following the day we receive the notice. If the Contract is terminated by us, the notice of termination shall become effective on the last day of the month following the month in which receive the notice, unless you are the Qualified Client, in which case we shall be entitled to terminate the Contract in accordance with the General Conditions;
b) As at the Conclusive Date;
c) Upon the blocking of the Certificate;
d) Upon the expiry of the Certificate.

6.2 Our right to cancel the Contract in accordance with the General Conditions shall not be prejudiced by this

FOR INFORMATION ONLY

provision.

6.3 You 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:

"**Authorisation SMS Message**" shall mean a message sent by the Bank to the Client at an agreed-upon GSM mobile telephone number operated by a Czech provider, by which the Client shall receive an SMS authorisation code. The SMS authorisation code shall be used for identifying the Client while using the relevant Banking Services, in particular MojeBanka and MojeBanka *Business* direct banking service, whereby the verification is made using a Personal Certificate stored in a data file.

"**Bank**" shall mean Komerční banka, a.s., registered office at Praha 1, Na Příkopě 33/969, Postal Code: 114 07, IČO (Company ID): 45317054, entered in the Commercial Register kept at the Municipal Court in Prague, section B, insert 1360.

"**Banking Services**" shall mean any banking deals, products and services provided by the Bank based upon its banking licence, including investment services provided by the Bank acting as a security broker/dealer.

"**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 depend, are open and provide the relevant services.

"**Certificate**" shall mean the Personal Certificate or Company Certificate issued under the Contract.

"**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 Bank's points of sale. This document is not a Notice as envisaged by the General Conditions.

"**Certification Wizard**" shall mean an application that supports and administers the Certificate. The Client may access the Certification Wizard on the Bank's Internet pages.

"**Client**" shall mean a natural person or legal person who has entered into the Contract with the Bank.

"**Client – Consumer**" shall mean a natural person who executes and performs the Contract for purposes not associated with his/her business or job activities, or a person requesting the provision of a Banking Service.

"**Client's Point of Sale**" shall mean the Bank's point of sale at which the Client has executed the Contract. The term "your point of sale" is used herein within the same meaning.

"**Company Certificate**" shall mean a Statutory Certificate issued by the Bank to a natural person (business) or a legal person under the Contract, which also contains the Private Key.

"**Conditions**" shall mean these Terms and Conditions Applying to Certificates, which are the Product Terms and Conditions within the meaning of the General Conditions.

"**Contract**" shall mean a contract under which the Bank issues a Company Certificate or Personal Certificate to the Client.

"**Decalogue of the Security**" 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 Security public on its Internet pages. It is also available at the Bank's points of sale. This document is not a Notice as envisaged in the General Conditions.

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

"**MojeBanka**" shall mean a direct banking service that the Client may use pursuant to a contract for the provision of direct banking services.

"**Notices**" shall mean communications in which further conditions and technical features of providing the Banking Services are specified in accordance with the General Conditions or relevant Product Terms and Conditions. The following document, without limitation to it, is not a Notice: 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).

"**Personal Certificate**" shall mean a Statutory Certificate issued by the Bank to a Client – Consumer under the Contract, which also contains the Private Key.

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

"**Private Key**" shall mean the data used for creating the Client's electronic signature.

FOR INFORMATION ONLY

"**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 Client's electronic signature.

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

"**Statutory Certificate**" shall mean a data message issued by the Bank to the Client under the Contract. The message links data for verifying the Client's electronic signature with the signatory and makes it possible to verify Client's identity when using the Services in accordance with Act No. 227/2000 Coll., on Electronic Signature, as amended. The Statutory Certificate contains the Public Key and Client's identification data.

"**Tablet**" shall be a mobile personal computer using a touch screen technology.

"**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 our Internet pages shall mean a reference to www.mojebanka.cz or other Internet addresses we currently use or shall use in association with providing the Banking Services.

Article 8. Final Provisions

8.1 We are entitled to amend these Conditions from time to time in the manner set forth in the General Conditions. We shall inform you about the amendment via the relevant direct banking service or in the manner specified in the General Conditions.

8.2 These Conditions repeal and replace the Terms and Conditions Terms and Conditions of the Issue and Use of a Personal and Company Certificate effective from 15 July 2017.

8.3 These Conditions come into effect as of 20 May 2018.

FOR INFORMATION ONLY