ELECTRONIC SIGNATURE & KB BANK IDENTITY TERMS AND CONDITIONS

These terms and conditions describe in detail the rights and duties arising from the Electronic Signature & KB Bank Identity Contract. Please read this document thoroughly. We shall gladly answer any of your questions.

Article 1. Electronic Signature Methods

1.1 **Methods.** You may use the following Methods for selected Banking Services, in particular when using the direct banking services:

- Certificate stored on a chip card,
- KB Key,
- Security Password.

We reserve the right to accept only certain Methods for certain Banking Services, including depending on the manner in which we have identified you. The respective Methods may be used for your authentication, confirmation of your will, and/or for the signing with the Electronic Signature. If we make it possible in specific cases, you may use certain Methods for the purpose of authentication, confirmation of your will, as well as the Electronic Signature also with respect of third parties.

1.2 Only you shall be entitled to use the Methods provided under the Contract.

1.3 You shall pay a fee as per the Tariff of Fees for the provision and use of the Methods and related services.

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

1.5 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 them and adhere to the principles contained therein.

1.6 You acknowledge that full functionality of the Methods is subject to compliance with the technical parameters specified in the Technical Terms and Conditions.

Article 2. KB Bank Identity

2.1 **KB Bank Identity.** The KB Bank Identity consists of a set of your identification data kept with us in connection with one of the above Methods, while each of the Methods establishes your unique KB Bank Identity. The KB Bank Identity is your electronic identity card, thanks to which your identity can be verified remotely.

2.2 **Using the KB Bank Identity while dealing with us.** You may use the KB Bank Identity to identify yourself when using the Banking Services and when communicating with us remotely. You can also use the KB Bank Identity to prove your identity to the Bank's Financial Group Members, as long as it is permitted by the relevant Bank's Financial Group Members and, if necessary, after fulfilling additional conditions set by them.

2.3 **Using the KB Bank Identity after registering in the National Point; consents to disclosing bank secrecy.** If your KB Bank Identity is registered with the National Point, the KB Bank Identity may also be used when your identity is proved to government/regional/local authorities, as well as to third parties outside the qualified electronic identification system within the meaning of the Act on Electronic Identification[2], specifically when using the services provided by these entities, if you are allowed to do so.

The identification services, which means identification, authentication, and trust services (for example, signing documents), using the KB Bank Identity with respect to third parties according to the previous sentence cannot be performed without your consent to disclosing bank secrecy, including your identification data and other information you allow to be disclosed, unless otherwise provided by law.

1 Act No. 89/2012 Coll., the Civil Code, as amended.

2 Act No. 250/2017 Coll., On Electronic Identification, as amended.

2.4 **Registering in the National Point.** We shall register your KB Bank Identity in the National Point in accordance with law[3] as soon as it is legally and technically possible. However, this only applies either to KB Bank Identities the holder of which is over 15 years of age or to KB Bank Identities for which a unique mobile phone number has been registered. We shall perform the registering not earlier than 14 calendar days from the effective date of the Contract; it may be performed earlier, though, if you initiate the use of a service that requires the registering. The registering includes verifying your identity through the National Point using your data, i.e. in particular, the number and type of your identity document, address of residence, date of birth, name, surname, place of birth, and citizenship. Subsequently, an identifier shall be assigned to your Bank Identity, which we shall enter in the National Point together with the identifier of the KB Bank Identity holder, the KB Bank Identity guarantee level and other parameters. After registering, you shall be obliged to check, via the MujProfil portal, the accuracy of the identification data that are part of your KB Bank Identity and that we keep about you.

2.5 **Prohibition and permission of registering in the National Point.** If you are not interested in registering your KB Bank Identity in the National Point or in the subsequent duration of the registering for the purpose of using your KB Bank Identity pursuant to Article 2.3 hereof, you shall be entitled to prohibit the registering or the subsequent duration thereof for the purpose of using your KB Bank Identity. If, following a previous prohibition, you want to either prohibit or permit the registering and use of the KB Bank Identity, you can do so at the MujProfil portal after your log in using your KB Bank Identity. The actual registering in the National Point and the use of the KB Bank Identity through the mediation of the National Point is based on the obligation imposed on us by law and by the Contract, not by virtue of your consent. However, you have the right to prohibit and subsequently permit the registering as described above.

2.6 **Applicable Methods.** You hereby acknowledge that, when using the KB Bank Identity to prove your identity to the entities referred to under Article 2.3 hereof, you may only use those Methods upon whose arrangement (or at any time later) your identification was performed at your presence or, as the case may be, legal requirements were fulfilled. At the same time, you acknowledge that for the purposes of the foregoing sentence, only the Methods can be used that can be registered in the National Point and that we shall have registered in this way. A list of the Methods used for this purpose can be found at our Internet pages.

2.7 **Security rules and liability for their violation.** The use of the KB Bank Identity is governed by the security rules set out in Article 8 hereof and in the Decalogue of the Security. Any failure to comply with the above obligations and recommendations may result in the misuse of your KB Bank Identity, even with respect to government authorities, or of confidential information, and to the possible occurrence of a harm on your side or on a side of a third party and, at the same time, to your liability for such harm. You shall be held liable for such harm at least until the moment you report to us, on the telephone number +420 955 551 552, the loss, theft or misuse (even suspected) of your KB Bank Identity or of the Method, a mobile telephone/device, access details or other confidential information; at the same time, it absolves us of all responsibility. You shall be obliged to report according to the foregoing sentence without any unnecessary delay after learning about the loss, theft, misuse or unauthorized use of your KB Bank Identity.

Article 3. Certificate Stored on a Chip Card

3.1 **Form of the Certificate**. The certificate (both commercial and qualified) shall be stored on a chip card we shall provide you with. You can arrange the chip card in a standard mode or in a QSCD mode. Upon receipt of the chip card containing the Certificate, you shall be obliged to check and verify the details contained in the Certificate, in particular your identification details (i.e., your name, type of the Certificate, email address, country of residence or domicile, and the chip card number). The Bank shall not be liable in the event that any incorrect or incomplete information is still contained in the Certificate after your confirmation

3.2 **Type of the Certificate**. You may choose a commercial or qualified Certificate when entering into the Contract. If you choose a qualified Certificate, a commercial Certificate shall be provided to you and stored on your chip card as well.

3.3 **Commercial Certificate**. You may create an electronic signature based on the Commercial Certificate, which is a guaranteed electronic signature within the meaning of the eIDAS Regulation.

3 Act No. 21/1992 Coll., On Banks, as amended; Act No. 250/2017 Coll., On Electronic Identification, as amended; Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

3.4 **Qualified Certificate**. Depending on the chip card mode, the qualified Certificate can be used to create a recognized electronic signature as envisaged in the Trust Services Act[4] in the form of a guaranteed electronic signature based on a qualified certificate for electronic signature or of a qualifies electronic signature. When creating a qualified electronic signature within the meaning of the eIDAS Regulation, you can only use qualified Certificate stored on a chip card in the QSCD mode. The qualified Certificate cannot be used for authentication.

3.5 **KB Signature Module**. You shall be obliged to follow our instructions and install the KB Signature Module to communicate with our chip card. This module handles all operations with the chip card, in particular, logging in, transaction authorization, and signing transactions and documents in the respective applications. The module also provides a secure environment for obtaining a negotiated Certificate using the MůjProfil portal. Further, the module allows you to change or unblock the chip card PIN.

3.6 **Activation**. Upon entering into the Contract and in cooperation with you, we shall send you a one-time password to the agreed GSM mobile telephone number so that you can create your commercial Certificate using the MůjProfil portal, or we shall create the Certificate, including the generation a Private and Public Key, and store it on a chip card at our point of sale. The one-time password shall remain effective for a period of 3 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 Codes. In the case of a qualified Certificate, the commercial Certificate must first be activated and, subsequently, you shall activate your qualified Certificate either at our point of sale or on the MůjProfil portal.

3.7 **Certificate policy**. Detailed rules and procedures for the use of the Certificate (both commercial and qualified) are set out in the Certificate Policy available on the Bank's website.

Article 4. KB Key

4.1 **Applications and equipment.** If we allow you to do so, you can activate the KB Key Method in several applications (e.g. in KB+ mobile telephone application or using the KB Key), even on multiple devices. You can use more than one application with the KB Key activated on the same device. By activating the application, the KB Key Method is also activated. We reserve the right to limit the number of active applications in which you can have the KB Method. The scope of functionality of the KB Key Method may vary from application to application. The validity of the KB Key Method shall not be limited in time. The KB Key Method is protected by a PIN code (i.e., a personal numerical code used to prove your authorisation to use the KB Key Method when operating the application). It is also possible to activate biometric PIN protection in the application. You can set a different PIN code in each application in which the KB Key Method activated. The application and the KB Key Method can be activated in one of the following manners.

4.2 **Applications downloads.** When downloading the applications that support using the Method on your devices, you may download them from trusted sources only (e.g., Google Play, Apple Store).

4.3 **Activation**. The activation shall take place at your request in the following manner, even in the case that even a minor's legal statutory representative requests the activation.
Activation using a QR code. You shall activate the application using a one-time QR code, which you can collect at our branch, generate at a KB's ATM, or get sent encrypted to your email, and a one-time password, which we shall send you via SMS to your contact number. You shall complete the activation by setting your PIN code directly in the application.
Activation using a one-time password. You shall activate the application by entering your identification number provided in the Method activation request and a one-time password we shall send you via SMS to your contact number. You shall complete the activation by setting your PIN code.
Each activation code and one-time password have a maximum validity period. After the expiry of the period you have to ask KB for resending.

4.4 **Duplicity.** The mobile telephone number you indicate in the Contract as that to which we should send the one-time password and 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 mobile telephone number or to which we should deliver the one-time password and/or Authorisation SMS Messages.

[4] Sect 6(2) of Act No. 297/2016 Coll., on Trust Services for Electronic Transactions.

ELECTRONIC SIGNATURE & KB BANK IDENTITY TERMS AND CONDITIONS

Article 5. Security Password

5.1 **Activation**. Upon entering into the Contract (or at any time thereafter, provided that you ask us to do so in an acceptable manner), we shall send you an SMS message to the agreed mobile telephone number, containing a one-time password for the activating of the Method. The one-time password shall remain effective for a period of 3 days from being sent to you. After the lapse of the aforesaid period, you should ask for the activation password to be sent once more.

5.2 We may not accept the mobile telephone number you indicate in the Contract as that to which we should send the one-time password and Authorisation SMS Messages if it has been used by another Client for the same purpose. We shall not be held liable for any damage caused by the fact that you might have stated a wrong mobile telephone number or to which we should deliver the one-time password and/or Authorisation SMS Messages.

5.3 When you use the Security Password Method for the first time, you shall activate it using your identification number stated in the application for the activation and the one-time password sent by an SMS message as per Article 5.1 hereof.

Article 6. Validity of the Respective Methods

6.1 **Validity of the Certificate.** The Certificate shall be valid for 2 years as a rule. The term of validity of a specific Certificate is specified in the Certificate itself or can be determined using the MůjProfil portal. You may use a valid and effective Certificate while utilising the Services. You also may ask for the renewal of the Certificate stored on a chip card before its expiry using the MůjProfil portal.

6.2 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.

6.3 If your identification data stated in the Contract (including the 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 Contract should change, you shall be obliged to notify us at a Bank's point of sale, or you can change your address having logged at MůjProfil portal.

6.4 **Validity of the KB Key & Security Password**. The validity of these Methods is not limited in time.

Article 7. Blocking and Deactivating the Methods

7.1 **Blocking and Deactivating.** If a Method is blocked, its validity shall be suspended until you ask us to unblock it. If a Method is deactivated, it is permanently terminated. You shall have to reactivate it so that you can use it again. We shall inform you about the blocking/deactivating of the Method on the contact telephone number specified in the Contract. If the Certificate stored on a chip card provided under the original Contract for the Certificate is blocked, the contract shall be automatically terminated. When a given Method is blocked or deactivated, the KB Bank Identity that is linked to the Method shall be disabled.

7.2 **Blocking on our part**. We shall be entitled to block the Method for as long as necessary, if it is necessary for serious reasons, in particular for security reasons (e.g. in case of suspected unauthorised or fraudulent use or in case of a tampered operating system). Once the reasons for blocking the Method no longer exist, we shall, with your cooperation, allow the Method to be unblocked or replaced by another Method.

7.3 **Blocking on your part**. You may request the blocking of a Method at any time via the Client Line, at any of our points of sale or using the MůjProfil portal on our Internet pages. You must request the blocking of a Method any time you suspect that the Method might have been misused.

7.4 **Deactivating on our part**. We shall deactivate the Method you use and possibly also shall demand that you apply for its reactivation 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 which form part of the Method is no longer valid,
- You are in breach of any of your duties under the Contract,
- The mobile telephone number to which 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 provide the given Method,
- We are 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.

7.5 **Deactivating on your part.** You may request the deactivation of the Method at any of our points of sale or on our Internet pages via the MujProfil portal.

7.6 For Certificates stored on a chip card, the chip card shall be blocked after the third incorrect PIN entry. You may ask for the chip card to be unblocked at any of our points of sale or can do it using the KB Signature Module and KB Cryptoplus software applications. In both cases, the PUK Code must be entered to unblock the chip card.

7.7 The KB Key Method used in a specific application on a given device and the Security Password Method shall be blocked after a given number of failed attempts.

7.8 We shall be entitled to limit the use of an application that uses the KB Key Method in a device if the operational system of such a device has been tampered with.

7.9 **Unblocking the Method.** If your Method has been blocked, you can request the unblocking through any of our points of sale, our ATMs, the KB+ mobile telephone application, or the MůjProfil portal, under the conditions set by us. If you wish to make full use of the KB Banking Identity using a method that has been unlocked remotely without your physical presence, we may require you to visit one of our points of sale in person. We reserve the right to alter the manner of unblocking the Method and of its subsequent use, especially depending on our technical capabilities or changes in law.

7.10 **Blocking and deactivating the KB Key Method in individual applications.** The KB Key Method can be blocked or deactivated as described in the previous articles. It can also be blocked or deactivated in individual applications on a specific device. If the KB Key Method is deactivated in the last application on the last device, the entire KB Key Method shall be deactivated.

7.11 **Device replacement.** If you request a device replacement in an acceptable manner, we shall deactivate the KB Key Method in all applications on the original device. On the new device, you must separately activate each application in which you want this Method to be active.

7.12 **Blocking and deactivating the Method 'Certificate stored on a chip card'**. If the chip card contains both a commercial Certificate and a qualified Certificate and this Method is blocked or deactivated, both Certificates shall be blocked or deactivated as a result. This shall not apply if this Method is blocked due to a change to the identification details that are part of the Method. In this case, only the qualified Certificate shall be invalidated. For the purposes of these Conditions, both blocking and deactivation of a Certificate shall mean invalidation of the Certificate. The invalidation shall take effect as soon as we execute it.

7.13 **Certificate validity information**. Under eIDAS, we shall be obliged to provide any relying party with information about the validity or invalidation of the Certificates we have issued.

Article 8. Security

8.1 **Security prior to activating the Method – loss or theft**. If the mobile telephone or the device 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 or the device to which the one-time password should be sent is lost or stolen prior to activating the Method, you shall be obliged to notify us without any unnecessary delay via the Client Line 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, as stated in the Contract, in the case of the Certificate.

8.2 **Certificate.** You 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 you have used for this purpose. Being the sole user of the Certificate including the Private Key, you shall be liable for their use.

8.3 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.

8.4 You shall be obliged to protect your 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, 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 Electronic Signature. You must continuously make sure that the Certificate has not been lost, stolen, misused or used without authorisation.

8.5 **Loss of the chip card.** If the chip card on which the personal certificate is stored is lost, or if the chip card security features are lost, you shall be obliged to notify us without any unnecessary delay to the above telephone number and apply for blocking the personal certificate.

8.6 **KB Key.** The KB Key Method is PIN protected. You can set different PINs on different devices for each application with the KB Key Method activated. You must protect these PINs and not disclose them to third parties. You are also obliged to protect your devices on which the Method is activated and not to allow third parties to access or use them. You must protect the one-time passwords used to activate the Method in the same manner.

8.7 You must notify us without any unnecessary delay of the loss, theft or any misuse (even suspected) of any of the Methods or the password, PIN or PUK Codes, and ask us to block the specific Method.

8.8 **KB Key; Security Password**. When you are logging in using these Methods, we may ask you to enter your contact telephone number as specified in the Contract for further authentication in addition to entering the PIN code and other security features.

Provisions Applicable to All Methods

8.9 You shall discharge your duty to inform us pursuant to these Conditions through any of our points 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 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, it shall be construed as if we have not been notified without any unnecessary delay.

8.10 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. 128/2005 Coll., on Electronic Communications, as amended.

8.11 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 Method resulting from misuse of a PC or another device you use (e.g. caused by software supplied by another supplier, a virus infected PC, hardware fault etc.).

8.12 We shall not be held liable for cases where the Method 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.

8.13 **General obligations.** In case of (even suspected) loss, theft or misuse of your (i) KB Bank Identity or (ii) your Security Data and features you shall be obliged to notify us of this fact without any delay and to request that the relevant Method be blocked.

8.14 You shall be obliged to protect your Security Data and Features, in particular from possible loss, disclosure, theft or unauthorised use and the like.

You further undertake to take any necessary steps to protect the direct banking system, your device and/or the KB Bank Identity from any misuse by third parties. In particular, you are not allowed to store other persons' identification elements in your portable device if you use a fingerprint reader or face recognition technology, or to allow any third person to store his/her identification elements in your device. The foregoing shall accordingly apply also to other technologies that we shall accept and that may allow for identifying a portable device's owner on the operating system level. You acknowledge that when entering your login details while logging in your internet banking application, you may only use the Internet address www.login.kb.cz.

For access via applications PSD2 provided by licensed third parties, redirection from these applications is permitted, however only to any of the above websites for entering your login details.

Any breach of this obligation shall be considered to be gross negligence. We shall not be liable for any damage caused to you as a result of your login details being entered into your internet banking account via a different internet address than stated above or to a different Internet address than stated above.

As a result of such gross negligence, you shall be fully liable for any and all damages caused to you by third parties until the moment a loss, theft, or misuse of your Security Data and Features is demonstrably reported.

8.15 **Further responsibility to ensure the safety of your device.** When operating your device you shall be obliged to use an antivirus programme and update it regularly; use an updated operating system and an updated Internet browser; visit only known websites; not to download or install programmes from untrusted sources; not to use compromised (e.g. jailbroken or rooted) mobile devices; use a trusted and properly secured device; only download apps to your smartphone from official sources (e.g. Google Play, Apple Store, Windows Phone Store); use a password that is not too simple, easily guessed or deducible from your personal data; check your device constantly; not to disclose your access details to a third party; not to write them down in an easily recognizable form or keep/carry them together with the device; not to allow password saving in a web browser; not to enter your sensitive data over the internet without reason; not to open suspicious e-mail attachments or files with unknown content; not to respond to suspicious e-mail messages, especially to requests for passwords, PIN codes, payment card numbers, etc., or click on links in such e-mail messages and e-mails. You can check the authenticity of an email sent from KB by referring to the Rules for Sending Electronic Communications, which you can find in the Decalogue of the Security. You are also obliged to protect the device you use for Internet Banking or on which you have activated the Method from misuse by a third party; to only use your computer or mobile telephone when logging into Internet Banking; to decline a request and to contact us immediately if a login or transaction request that you have not entered appears in the KB Key; to monitor your Internet Banking login history; and to check your transaction history regularly.

8.16 **Your liability.** We shall hold you liable for any damage we may suffer in case that you breach your duties set forth herein.

8.17 We shall be entitled to collect anonymous data and information related to your use of the Methods for security reasons, in particular in order to prevent any possible misuse of these Methods. At the same time, we shall be entitled to restrict the sending of the Authorisation SMS Messages and one-time passwords.

8.18 In accordance with the Commission Delegated Regulation (EU) 2018/389, we apply a transaction tracking mechanism to detect unauthorized or fraudulent payment transactions. As part of your login to the following services of direct banking: MojeBanka, MojeBanka Business, Profibanka and Mobilní banka, we process and evaluate data concerning your device, browser and ongoing connection in order to identify signs of malware infection. Processing is done using the ThreatMark Anti-Fraud Suite component provided by ThreatMark (Company ID: 04222091), which processes your personal data for us. The data shall be kept in order to identify and evaluate potential threats. For more information on the processing of personal data, see the Information on the processing of personal data for our clients published on our website.

8.19 If you sign an electronic document using the KB Key Method or the Security Password Method, our server certificate shall be attached to the electronic document and the so-called remote signing shall take place in the form of the "Server Side Signing" service. Thus, the person acting and the content of the legal proceedings are captured, and the maintaining of the integrity of the records stored in our electronic information system is objectively assured. Our server certificate is attached automatically.

8.20 The statutory representatives of minor users who are a party to the Contract shall be obliged not to use or misuse the Direct Banking system, equipment, or KB Banking Identity issued to such minor users. In the event of a breach of this obligation, the statutory representative shall be liable not only to the minor user, but also to us and to third parties.

ELECTRONIC SIGNATURE & KB BANK IDENTITY TERMS AND CONDITIONS

Article 9. Termination of the Contractual Relationship

9.1 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 period shall be 2 months, unless we specify a longer period in the notice, and shall start at the moment of then delivery of the notice. The original Contract for the Certificate shall expire automatically upon the expiry of the Certificate;

b) As at the Conclusive Date;

c) If you terminate the Contract for Opening and Maintaining an Account while switching a payment account under applicable law[5], the Contract shall be terminated as at the date on which this payment account ceases to exist, unless we still maintain another payment account for you at the same time;

d) Starting from 18 July 2023, 24 months from the date of the execution of the contract under which the Method has been provided to you (whether or not it shall have been activated) or from the date of the last use of the Method, always provided that you have not effectively used any of your Methods with respect to us or any third party to make authentication, authorisation, or electronic signature during such period of time;

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

9.3 You shall not be allowed to use any of the Methods after the expiry/termination of the Contract.

Article 10. Definition of Terms

10.1 Capitalised terms used herein shall have the meaning assigned to them in the General Conditions, or the following meaning:

"**Authorisation SMS Message**" shall mean a message sent by the Bank to the Client to an agreed-upon (GSM) mobile telephone number operated by a Czech provider (and also by a foreign provider in case of a chip card), 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 or MojeBanka Business Internet Banking.

"**Bank**" shall mean our company, 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, services and products provided by the Bank based on 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 depends, are open and provide the relevant services.

"**Certificate**" shall mean a Method consisting in a personal certificate stored on a chip card that makes it possible, above all, to verify the signatory's identity, sign documents electronically, and authorise payment transactions. It contains the Public Key, Private Key and Client's identification data. The certificate may be either commercial or qualified at the Client's choice.

"**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 Internet pages. The Certification Policy is also available at Bank's points 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 Client's authorisation to handle the chip card.

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

"**Client Line**" shall be the round-the-clock telephone hotline at the number +420 955 551 552 (for calls in the Czech Language) and +420 955 551 556 ("Customer Service KB" for calls in the English language). The telephone number is available at the Bank's points of sale and at its Internet pages. The Bank shall notify the Client of a possible change to the telephone number well in advance.

5 Act No. 370/2017 Coll., on Payment System, as amended.

"**Conditions**" shall mean these Electronic Signature & Bank Identity Terms and Conditions, which are the Product Terms and Conditions within the meaning of the General Conditions.

"**Contract**" shall mean a contract under which the Client arranges the Method(s).

"**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.

"**eIDAS**" shall mean 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, regulating in particular electronic signatures and electronic identity.

"**Electronic Signature**" shall mean an electronic signature within the meaning of eIDAS based on the Methods we make available to you under the Contract.

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

"**KB Key**" shall mean a Method that is based on individual properties of an activated application for supported portable devices and on a knowledge of a security PIN code or on biometry, which makes it possible, above all, to verify the signatory's identity, sign documents electronically, and authorise payment transactions.

"**KB Key PIN**" shall mean a personal numeric code used to verify the eligibility to handle the application enabling the use of the KB Key Method.

"**KB Signature Module**" is a software add-on that is installed as part of the software enabling secure use of the KB Certificate and its management in direct banking services or on the MyProfil portal.

"**Method**" shall mean an Electronic Signature creation method and KB Banking Identity creation method agreed upon under the Contract.

"**MojeBanka***"* shall mean Internet Banking, which the Client may use pursuant to a contract for the provision of direct banking services.

"**MůjProfil**" shall mean a portal for the support and management of the Methods. Můj Profil is accessible to the Client on the Bank's Internet pages, to which the Client may log in using any Method or directly from our Internet Banking, as long as it is allowed.

"**National Point**" is a public administration information system supporting the process of electronic identification and authentication, administered by the Administration of Basic Registers.

"**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 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).

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

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

*"**QSCD**" (Qualified Signature Creation Device) is a specific type of computer hardware that must meet rigorous technical requirements, has been certified by a qualified trust service provider, and is used in creating a qualified electronic signature within the meaning of the eIDAS Regulation.*

"**Security Data and Features**" shall mean such data and features that are confidential and need to be protected and that may cause you damage if disclosed. These include the Method itself, the password, PIN, PUK, one-time activation password, SMS OTP if applicable, the QR code provided, your login ID, user name and, other access data, as well as the computing system itself including mobile devices.

"**Security Password**" shall mean a Method that is based on creating a security password for web applications consisting of a string of characters, which is known only to the Client and makes it possible, above all, to verify the signatory's identity, sign documents electronically, and authorise payment transactions.

"**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 parameters 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.

10.2 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 11. Final Provisions

11.1 Wherever the contracts and other documents entered into by and between you and us, or the contractual documents that are part of such contracts, refer to the Terms and Conditions Applying to the Electronic Signature or the Electronic Signature Contract, this shall mean the Electronic Signature & KB Bank Identity Terms and Conditions or the Electronic Signature & KB Bank Identity Contract.

11.2 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.

11.3 These Conditions repeal and replace the Terms and Conditions Applying to the Electronic Signature effective as of 30 October 2022. At the same time, these Conditions repeal and replace the Terms and Conditions applying to Certificates issued by the Bank and connected to the Contract for the Certificate effective as from 07 January 2024.

11.4 These Conditions come into effect as of 16 April 2024.