ELECTRONIC SIGNATURE AND KB BANK IDENTITY TERMS AND CONDITIONS

These terms and conditions provide a more detailed regulation of the rights and obligations following from the concluded Agreement on Electronic Signature and KB Bank Identity Please familiarise yourself thoroughly with this document. We will be happy to answer any questions you may have.

Article 1. Electronic Signature Methods

1.1 **Methods.** You can use the following Methods for selected Banking Services, especially when using direct banking services:

- Certificate on Chip Card;
- KB Klíč;
- Security Password.

We reserve the right to accept only certain Methods for certain Banking Services, depending on how we have identified you. The individual Methods may serve for your authentication, confirmation of your manifestation of will or the use of your Electronic Signature. You may also use certain Methods for your authentication, confirmation of your manifestation of will and your Electronic Signature *vis-à-vis* third parties if we allow you to do so in a particular case.

1.2 Only you personally can use the Methods.

1.3 You pay the prices for the provision and use of the Methods and related services according to the applicable List of Fees.

1.4 This Agreement will be governed by the laws of the Czech Republic, in particular the Civil Code[1].

1.5 By signing the Agreement, you confirm that you have familiarised yourself with the contents and meaning of the Certification Policy and the Ten Security Principles, and you agree to comply with them and adhere to the principles set out therein.

1.6 You acknowledge that the full functionality of the Methods is conditional on compliance with the technical parameters set out in the Technical Terms and Conditions.

Article 2. KB Bank Identity

2.1 **KB Bank Identity.** Your KB Bank Identity is a set of your identification details registered with us in connection with one of the Methods listed above, where each Method establishes your unique KB Bank Identity. The KB Bank Identity is your electronic identity card which enables us to verify your identity remotely.

2.2 **Use of the KB Bank Identity *vis-à-vis* us**. The KB Bank Identity serves to identify you when you are using our Banking Services and when you communicate with us remotely. You can also use the KB Bank Identity to verify your identity *vis-à-vis* Members of the Bank's Financial Group, if the relevant Members of the Bank's Financial Group allow this and, where applicable, subject to additional conditions set by them.

2.3 **Use of the KB Bank Identity after registration with the National Point and consents to the waiver of banking secrecy.** If the KB Bank Identity is registered with the National Point, the KB Bank Identity may also serve for your identification *vis-à-vis* governmental authorities and bodies of territorial self-governing units, as well as *vis-à-vis* third parties outside the scope of the qualified electronic identification system within the meaning of the Electronic Identification Act,[2] when using the services of these entities, if they allow you to do so.

The identification services, i.e. identification, authentication and trust services (e.g. also the signing of documents) via the KB Bank Identity can be used *vis-à-vis* third parties pursuant to the preceding sentence only with your consent to the waiver of banking secrecy, including the identification and other details approved by you, unless the legal regulations provide otherwise.

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

2 Act No. 250/2017 Coll., on electronic identification, as amended

2.4 **Registration with the National Point**. As soon as legally and technically possible, we will register your KB Bank Identity with the National Point in accordance with the legal regulations[3]. This applies only to KB Bank Identities where the holder is over 15 years of age and to KB Bank Identities with a registered unique mobile telephone number. We will register you in each case not sooner than upon expiry of 14 calendar days of the effective date of the Agreement, or sooner if you initiate the use of a service that requires registration. The registration includes verification of your identity via the National Point using your identification details, i.e. in particular the number and type of identity document, address of residence, date of birth, name, surname, place of birth, and citizenship. Your Bank Identity will then be assigned a KB identifier, which we will enter into the National Point together with the KB Bank Identity holder's identifier, the KB Bank Identity guarantee level and other parameters. After the registration, you are required to check, via the MůjProfil portal, the accuracy of the identification details that form part of your KB Bank Identity and that we record on you.

2.5 **Prohibition and permission to register with the National Point.** If you are not interested in the registration of your KB Bank Identity with the National Point or in the continuation of the registration for the use of your KB Bank Identity pursuant to Art. 2.3, you have the right to prohibit the registration or subsequent continuation of the registration for the use of the KB Bank Identity. You can prohibit the registration and use of the KB Bank Identity or permit it following your previous prohibition on the MůjProfil portal after logging in with the KB Bank Identity. The actual registration with the National Point and the use of the KB Bank Identity via the National Point is based on an obligation imposed on us by the legal regulations and the Agreement, not on your consent. However, you have the right to prohibit and subsequently permit the registration in the above-specified manner.

2.6 **Applicable Methods**. You acknowledge that, to identify yourself via the KB Bank Identity *vis-à-vis* the entities referred to in Art. 2.3, you may only use Methods in respect of which you were identified in your physical presence at the time of their arrangement or at any time later, or if the legal prerequisites have been met. At the same time, you acknowledge that only those Methods that can be registered with the National Point and that we will register as such can be used for the purposes according to the preceding sentence. The list of applicable Methods for these purposes can be found on our website.

2.7 **Security rules and liability for their breach**. The security rules set out in Article 8 of these Terms and Conditions and in the Ten Security Principles apply to the use of the KB Bank Identity. Non-compliance with the obligations and recommendations specified above may result in the misuse of your KB Bank Identity, also *vis-à-vis* governmental authorities, or confidential information, and may result in harm incurred by you or by a third party, and may also result in your liability for any such harm. You are liable for any damage thus incurred at least until the time you report at +420 955 551 552 (even if only suspected) loss, theft or misuse of your KB Bank Identity or an Electronic Signature creation method, your mobile phone / device or access data or other confidential information, which also excludes our liability. You are required to make the report pursuant to the preceding sentence without undue delay after discovering the loss, theft, misuse or unauthorised use of your KB Bank Identity.

Article 3. Certificate on Chip Card

3.1 **Certificate form.** A Certificate (both commercial and qualified) will be stored on a chip card provided to you. You can arrange for a chip card in the standard mode or in the QSCD mode. Upon receipt of a chip card containing the Certificate, you are required to check and verify the data included in the Certificate, in particular your identification details comprising your name and surname, type of Certificate, email address, country of permanent or temporary residence, and the chip card number. The Bank is not liable if you provide incorrect or incomplete information which will form the contents of the Certificate once it is confirmed by you.

3.2 **Certificate type.** When entering into the Agreement, you may choose a commercial or qualified Certificate. If you choose a qualified Certificate, a commercial Certificate will also be provided and stored on your chip card.

3.3 **Commercial Certificate.** You can use a commercial Certificate to create an electronic signature that will be deemed a guaranteed electronic signature within the meaning of the eIDAS Regulation.

3.4 **Qualified Certificate.** Depending on the chip card mode, a qualified Certificate can be used to create a recognised electronic signature within the meaning of the Trust Services Act4 in the form of a guaranteed electronic signature based on a qualified certificate for electronic signature or a qualified electronic signature. Only a qualified Certificate on a chip card in the QSCD mode can be used to create a qualified electronic signature within the meaning of the eIDAS Regulation. A qualified Certificate cannot be used for authentication.

---

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 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

4 Section 6 (2) of Act No 297/2016, on trust services for electronic transactions.

3.5 **KB Signature Module**. Based on our instructions, you are required to install the KB Signature Module for communication with our chip card. The module handles all operations with the chip card, in particular login, transaction authorisation and signatures relating to transactions and documents in the respective applications. The module also provides a secure environment for obtaining the agreed Certificate via the MůjProfil portal, and the module can also be used to change the PIN code or unblock the chip card PIN code.

3.6 **Activation.** After the conclusion of the Agreement, we will send you a one-time password via an SMS to the agreed mobile phone number so that you can create a commercial Certificate through the MůjProfil portal, or we will create a Certificate for you at our point of sale, including the generation of the Private Key and the Public Key, and store it on a chip card. The one-time password is valid for a period of three days after it is sent. At the same time, we will give you the chip card and an envelope with a PIN and PUK code. In the case of a qualified Certificate, a commercial Certificate must first be activated; you can then use the latter to activate the qualified Certificate either at our point of sale or on the MůjProfil portal.

3.7 **Certification Policy.** Detailed rules and procedures in the use of a Certificate (whether commercial or qualified) are laid down in the Certification Policy available on the Bank's website.

Article 4. KB Klíč

4.1 **Applications and devices**. If we allow you to do so, you can activate the KB Klíč Method in various applications (e.g. in the KB+ mobile application or in the KB Klíč mobile application), even on multiple devices. You can have multiple applications with the KB Klíč activated on the same device. An activation of the application also activates the KB Klíč Method. We reserve the right to limit the number of active applications where you can have the KB Klíč Method. The range of functionalities of the KB Klíč Method may vary from application to application. The validity of the KB Klíč Method is not limited in time. The KB Klíč Method is protected by a PIN code (personal numeric code used to verify the authorisation for the application using the KB Klíč Method). You can also activate biometric PIN protection in the application. You can set a different PIN code in each application with the KB Klíč Method activated. The application and the KB Klíč Method can be activated in the ways specified below.

4.2 **Application download.** You are obliged to download application to use the Method only from trusted sources (e.g. Google Play, Apple Store).

4.3 **Activation.** The activation, even where a legal representative requests activation for a minor, takes place on your request in the manner specified below.

Activation by QR code. Activation can be done using a one-time code or QR code and a One-time Password; you can ask for the one-time code or QR code at our branch, generate it at a KB ATM (only for the KB Klíč application) or in the KB Klíč application, or receive it from us via your email in an encrypted form; the One-time Password will be sent via SMS to your contact telephone number. You will complete the activation by setting the PIN code directly in the application.

Each activation code and One-time Password always have a set maximum period of validity. After expiry of this period, you must ask us to resend it.

4.4 **Duplicity.** The mobile phone number for sending the one-time password and Authorisation SMS, which co-creates your KB Bank Identity and which you provide in the Agreement, cannot be used for the same purposes by another Client. We are not liable for any damage caused by providing an incorrect mobile phone number for the delivery of a one-time password or Authorisation SMS.

Article 5. Security Password

5.1 **Activation.** If you request us to activate your Security Password in an accepted manner, activation can be done using a one-time code; you can ask for the code at our branch, generate it at a KB ATM or receive it from us via your contact email in an encrypted form. You will enter your identification number and one-time code when you first log into your internet banking or the MůjProfil portal and then enter the One-time Password, which will be sent to you via SMS to your contact telephone number. It is also possible to activate the Security Password Method in the MůjProfil portal using the KB Klíč or a Certificate on a chip card. You will complete the activation by setting the password. The validity of the Security Password is not limited in time. Each activation code and One-time Password always have a set maximum period of validity. After expiry of this period, you must ask us to resend it.

5.2 We need not accept the mobile phone number you provide in the Agreement for sending the One-time Password if it has already been used for the same purpose by another Client. We are not liable for any damage caused by providing an incorrect mobile phone number for the delivery of a one-time password.

5.3 The first time you use the Security Password method, you activate it using your identification number provided in the activation request and the One-time Password sent via SMS pursuant to Art. 5.1.

Article 6. Validity of the individual Methods

6.1 **Validity of the Certificate.** The Certificate is generally valid for a period of two years. The specific period of validity of the Certificate is indicated in the Certificate or accessible via the MůjProfil portal. A valid and effective Certificate may be used for using the Services. Before the expiry of the Certificate on a chip card, you can apply for its renewal via the MůjProfil portal.

6.2 If you request a renewal of your Certificate before its expiry, we will issue a new Certificate to you based on the already concluded Agreement. The new Certificate will be issued in the same form as the previous Certificate, with the same notification details. You must not use the previous Certificate once a new one has been issued. The procedure under Article 3 of the Terms and Conditions shall apply *mutatis mutandis* to the issuance of a new Certificate.

6.3 If your identification details specified in the Agreement (including the mobile phone number agreed for sending One-time Passwords) change, you are obliged to inform us in writing without undue delay and also enter into an amendment to the Agreement with us or ask us to issue a new Certificate. If your email address specified in the Agreement changes, you must inform us at the Bank's point of sale or by changing the data after logging into the MůjProfil portal.

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

Article 7. Blocking and deactivating Methods

7.1 **Blocking and deactivating**. If a Method is blocked, its validity will be suspended until you ask us to unblock it. If a Method is deactivated, it is completely terminated. If you want to use it again, you must reactivate it. Information on the blocking or deactivation of the relevant Method will be sent to the contact telephone number specified in the Agreement. In the case of a Certificate on a chip card provided on the basis of the original Certificate Agreement, blocking or deactivating the Certificate will automatically terminate the Agreement. Blocking or deactivating a Method will disable the KB Bank Identity linked to that Method.

7.2 **Blocking on our initiative.** We are authorised to block a Method for the necessary period of time if this is required for serious reasons, especially security reasons (e.g. in case of suspected unauthorised or fraudulent use of the Method or a modified operating system). Once the reasons for blocking the Method cease to exist, we will allow you to unblock the Method or replace it with a different one. In some cases, we reserve the right to unblock the Method even without your assistance.

7.3 **Blocking on your initiative**. You can ask for a Method to be blocked at any time via the Client Hotline, at any of our points of sale or on our website via the MůjProfil portal. You must always ask for a Method to be blocked if you suspect that it may have been misused.

7.4 **Deactivation on our initiative**. We will deactivate a Method and, if applicable, require you to request its reactivation if:

- the Method was arranged on the basis of untrue, incomplete or misleading information;
- the identification details that form part of the Method are no longer valid;
- you have breached any obligation following from the Agreement;
- the same mobile phone number for sending the One-time Password has been agreed in multiple Agreement and/or for multiple Clients;
- we stop providing the Method;
- we are obliged to do so in view of the legal regulations;
- the security risks or measures related to an incorrect entry of security data or the use of the Method have increased or may increase.

7.5 **Deactivation on your initiative**. You can ask for a Method to be deactivated at any of our points of sale, via the Client Hotline, in your KB Klíč application or on our website via the MůjProfil portal.

7.6 In the case of the Certificate on Chip Card Method, the third incorrect PIN code entry will lock the chip card. You can ask us to unblock the chip card at any of our points of sale or use the KB Signature Module and Cryptoplus KB software to do so. In both cases, you must provide the PUK code to unblock the chip card.

7.7 We also have the right to temporarily block all your Methods if a certain set number of consecutive incorrect login attempts are made by any of your Methods. We will unblock the Methods automatically without your co-operation after expiry of the blocking period set by us.

7.8 We are authorised to restrict the use of an application with the KB Klíč Method on a device whose operating system has been modified.

7.9 **Unblocking a Method**. If a Method has been blocked, you can ask for its unblocking through any of our points of sale, our ATM, the KB+ mobile application, your KB Klíč application or the MůjProfil portal, under the conditions specified by us. For the full use of the KB Bank Identity via a KB Method which has been unblocked remotely without your physical presence, we may require that you come personally to any of our points of sale. We reserve the right to change the ways of unblocking a Method and its subsequent use, especially depending on our technical capabilities or changes in the legal regulations.

7.10 **Blocking and deactivating the KB Klíč Method in individual applications**. The KB Klíč 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. When the KB Klíč Method is deactivated in the last application on the last device, the entire KB Klíč Method is deactivated thereby.

7.11 **Replacement of a device**. If you want to replace a device with another one, e.g. you have a new mobile phone, you must activate the KB Klíč Method on the new device as described in these Terms and Conditions and, if you no longer intend to use the old device, deactivate the KB Klíč Method on the old device as described in these Terms and Conditions.

7.12 **Blocking and deactivating the Certificate on Chip Card Method**. If the chip card contains both a commercial Certificate and a qualified Certificate, and this Method is blocked or deactivated, both these Certificates will be blocked or deactivated, as the case may be. This does not apply if this Method is blocked due to a change in the identification details included in this Method. In such a case, only the qualified Certificate will be invalidated. For the purposes of these Terms and Conditions, the blocking and deactivation of a Certificate means rendering the Certificate invalid. The invalidation takes effect immediately after it is performed.

7.13 **Information on the validity of the Certificate.** Under the eIDAS Regulation, we are required to provide any relying party with information on the validity or invalidity of Certificates we have issued.

Article 8. Security

8.1 **Security before activation of a Method – loss, theft.** In the case of a loss of theft of your mobile phone or device or a misuse or inaccessibility of the email address used to deliver the One-time Password before the Certificate is created, or a loss or theft of the mobile phone or device used to deliver the One-time Password before a method is activated, you must notify us immediately via the Client Hotline and arrange with us an alternative method of delivering a new One-time Password. We will then block the original One-time Password. In the case of a Certificate, we may use your email address specified in the Agreement for substitute delivery of the One-time Password.

8.2 **Certificate.** You are responsible for the Certificate creation process, including the generation of the Public Key and the Private Key on the computer used by you for this purpose. You are the exclusive use of the Certificate, including the Private Key, and as such you also responsible for its use.

8.3 The Private Key stored in the data file is protected by a password. The Private Key stored on the chip card is protected by the PIN code.

8.4 For the entire period of validity of the Certificate you are obliged to protect your Private Key and password, or PIN and PUK, as applicable, intended for use of the Private Key, in particular, against loss, disclosure to a third party, modification or unauthorised use. You must not store the password, or PIN and PUK, as applicable, intended for use of the Private Key, in the same place or on the same medium as the Private Key, and you must never store them in a manner accessible to third parties. In particular, you must never leave an unsecured Private Key on your computer in a state where the password is entered and the key is activated, or the chip card inserted in the chip card reader at a time when you are not logging into the relevant Banking Service or using Electronic Signature. You must regularly monitor for loss, theft, misuse or unauthorised use of the Certificate.

8.5 **Loss of chip card**. If the chip card with the personal certificate is lost or the security features to the chip card are lost, you are obliged to inform us immediately at the above telephone number and request the blocking of your personal certificate.

8.6 **KB Klíč.** The KB Klíč Method is protected by a PIN code. You can set different PIN codes for each device on which the application with the KB Klíč Method is activated. You must protect these PIN codes and not disclose them to third parties. Furthermore, you are obliged to protect your devices on which the Method is activated and not allow their access or use by any third party. The One-time Passwords used to activate this Method must be protected in the same way. You are required to reject the request and contact us immediately if you receive a request in the KB Klíč to log in or authorise a transaction that you have not entered (e.g. a request to make a payment or add or replace the mobile device); You are also required to carefully read all the requests or messages sent to you via KB Klíč, and not to confirm them unless you have entered them yourselves or in co-operation with a bank employee.

8.7 In case of (even suspected) loss, theft or misuse of any of the Methods or the password, PIN or PUK code, you must notify us immediately.

8.8 **KB Klíč, Security Password**. For the purposes of additional authentication when you log in using these Methods, we may require you to enter your contact telephone number as specified in the Agreement in addition to your identification number, PIN code and other elements.

Joint provisions.

8.9 You may perform your information obligations under these Terms and Conditions *vis-à-vis* us through any of our points of sales, electronically at an address listed in the relevant Product Terms and Conditions or via the above telephone number. If you fail to perform your information obligation within three Business Days from the date on which the obligation arose without being prevented from doing so by reasons of special consideration, the information obligation will be deemed not to have been performed without delay.

8.10 The electronic communication networks (public telephone lines, mobile network lines, email and fax) used for our mutual communication under the Terms and Conditions are not under our direct control; therefore, we are not liable for any damage incurred by you as a result of their misuse. The protection of these networks and the confidentiality of the transmitted messages shall be ensured by the relevant electronic communications service providers, in particular within the meaning of Act No. 127/2005 Coll., on electronic communications, as amended.

8.11 We are not liable for any unauthorised or incorrectly executed payment transactions, or for any damage you may have incurred in case of breach of your obligations set out in the Terms and Conditions, or for any damage incurred as a result of an incorrect authorisation or non-execution of an Order for reasons attributable to you or the payee. We are not liable for any misuse of the Method that occurs as a result of misuse of the computer or other device you are using (e.g. by a third-party program, computer virus, hardware malfunction, etc.).

8.12 We are not liable for cases where the Method cannot be used for reasons beyond our control or beyond the control of our partners (power outage, interruption of connection via the public telephone network, public internet network, strike, etc.). If you are not a Qualified Client under the GTC, we are not obliged to prove to you that a procedure was followed which enables us to verify that an Order has been given, that the payment transaction was authorised, correctly recorded, and posted, and that it was not affected by a technical failure or some other defect.

8.13 **General obligations.** Immediately upon becoming aware or suspicious of the loss, theft or misuse of your (i) KB Bank Identity, (ii) Security Data and Security Features, you are obliged to notify us and request the blocking of the relevant Method.

8.14 You are required to protect the Security Data and Security Features, in particular against loss, disclosure, theft or misuse.
You further agree to take measures to prevent misuse of the direct banking system, your device or KB Bank Identity by a third party. In particular, if you use a fingerprint reader or facial recognition technology on your mobile device, you may only save your identification elements on the device and you may not allow a third party to add their identification elements to the device. This applies similarly to any other operating-system level identification of the mobile device owner that we accept. You acknowledge that only the internet address https://login.kb.cz can be used to enter your login details into your internet banking. Enter this address directly. Do not use any search engines to find it. If you log into the internet banking via KB Klíč, you are obliged to verify that the alphanumeric verification code displayed in the KB Klíč corresponds to the code on the login screen.
Redirection from PSD2 licensed third-party applications is permitted for access via such applications, but in only to any of the above addresses for entering your login details.
A breach of this obligation will be deemed gross negligence, and we are not liable for any damage incurred by you if your login details are entered into your internet banking through an internet address other than the above or to an internet address other than the above.
As a result of such gross negligence, you are fully liable for any and all damage caused to you by third parties until you demonstrably notify us of the loss, theft or misuse of your Security Data and Security Features.

8.15 **Other responsibilities to ensure the safety of your device.** When using your device, you must: use and regularly update antivirus software, use an up-to-date operating system and web browser, access only trusted sites, not download or install software from unreliable sources, not use a mobile device with modified system settings (e.g. jailbreak or root), use only trusted and properly secured device, download applications only from official sources (e.g. Google Play, App Store), use a password that is sufficiently strong and not deductible from personal data, regularly monitor your device, not disclose your access details to a third party nor record them in an easily recognizable form or store or carry them together with your device, not allow your password to be saved in your web browser, not enter sensitive data online unless necessary, not open attachments of suspicious emails or files with unknown content, not respond to suspicious email messages, especially those requesting passwords, PIN codes, credit card numbers or similar information, not click on links in such messages and emails. You can verify the authenticity of an email sent from KB in the Rules for Sending Electronic Communications, which can be found in the Ten Security Principles. Furthermore, you must also protect the device you use for internet banking or on which the Method is activated against misuse by a third party, use your own computer or mobile phone to log into your internet banking, reject any login or transaction request received in KB Klíč that you did not initiate and contact us immediately, regularly monitor your internet banking login history and regularly review your transaction history.

8.16 **Your liability**. You are liable to us for any damage we incur as a result of the breach of your obligations under the Terms and Conditions.

8.17 For security reasons, in particular, to prevent a potential misuse of the individual Methods, we may collect anonymous data related to your use of these Methods and we may also restrict the sending of One-time Passwords.

8.18 In accordance with Commission Regulation (EU) 2018/389, we apply a transaction monitoring mechanism to detect unauthorised or fraudulent payment transactions. As part of your internet banking login into the following direct banking services: MojeBanka, MojeBanka Business, Profibanka and Mobilní banka, we process and evaluate data about your device, browser and ongoing connection to identify any signs of malware. The processing is carried out using the ThreatMark Anti-Fraud Suite component provided by ThreatMark s.r.o. (Id. No.: 04222091), which is the processor of your personal data for us. The data are stored for the identification and assessment of any possible threats. For more information on personal data processing, see the Information on Personal Data Processing published for our clients on our website.

8.19 If you sign any electronic document using the KB Klíč Method or the Security Password Method, our server certificate will be attached to the electronic document and the document will be signed by means of the “Server Side Signing” service. This ensures that the identity of the acting person and the contents of the legal act are captured, and that the integrity of the records kept in our electronic information system is maintained in objective terms. Our server certificate is attached automatically.

8.20 Legal representatives of minor users who are a party to the agreement are obliged not to use or misuse the direct banking system, device or KB Bank Identity issued to such minor users. In the case of a breach of this obligation, the legal representative is liable not only to the minor user, but also to us and third parties.

ELECTRONIC SIGNATURE AND KB BANK IDENTITY TERMS AND CONDITIONS

Article 9. Termination of the contractual relationship

9.1 The Agreement terminates:

a) by a notice of termination by one of the Parties. Both you and we may terminate the Agreement at any time in writing without stating a reason. The notice of termination becomes effective *vis-à-vis* us on the Business Day following the day of its delivery. The notice period *vis-à-vis* you is two months, unless we specify a longer period in the notice, and commences upon delivery of the notice to you. The original Certificate Agreement will terminate automatically upon termination of the Certificate;

b) on the Decisive Date;

c) if you terminate the Account Agreement within a change of payment account under applicable law[5], on the date of termination of the payment account, unless we already maintain another payment account for you;

d) Effective from 18 July 2023, by expiry of two years from the time of execution of the Agreement under which the Method was provided to you (regardless of whether it was activated or deactivated) or from the date of its last use, provided that none of your Methods have been successfully used for authentication, authorisation or electronic signature towards us or any other entity.

9.2 This is without prejudice to our right to withdraw from the Agreement under the terms set out in the GTC.

9.3 After termination of the Agreement, you may not continue using any of the Methods.

Article 10. Definitions

10.1 The capitalised terms used in the Terms and Conditions have the respective meaning set out in the GTC or the following:

"**Security Features**" include, in particular, computer technology (e.g. computer, laptop) and mobile devices (e.g. mobile phone, watch, tablet), including software, chip card, payment card and other elements utilised for the use of banking services and Methods.

"**Security Data**" are data used to verify the Client, including, in particular, One-time Password, password, PIN, PUK, one-time code (QR code, control code), Touch ID, Face ID, your login identification number (ID), username, Private Key and other access details, payment card number and security CVV/CVC code.

"**Bank**" means Komerční banka, a. s., with its registered office in Prague 1, at Na Příkopě 33/969, Postal Code 114 07, Id. No: 45317054, registered in the Commercial Register kept by the Municipal Court in Prague, Section B, File 1360.

"**Banking Services**" mean any banking transactions, services and products provided by the Bank on the basis of the Bank's banking license, including investment services provided by the Bank as a securities trader.

"**Security password**" is a Method based on the creation of a security password for web applications, based on a string of characters known only to the Client and enabling, in particular, to verify the signatory's identity, to sign documents electronically and to authorise payment transactions.

"**Certification Policy**" is a document in which the Bank sets out the rules and procedures in the use of the Certificate and its specification, and which the Bank is authorised to change. The Bank publishes the Certification Policy on its website. The Certification Policy is also available at the Bank's points of sale. This document does not constitute a Notice within the meaning of the GTC.

"**Certificate**" is a Method in the form of a personal certificate stored on a chip card that allows, in particular, to verify the signatory's identity, to sign documents electronically and to authorise payment transactions. It contains the Public Key, Private Key and the Client's identification details. The Certificate may be commercial or qualified according to the Client's choice.

"**Ten Security Principles**" means the Ten Security Principles for the use of Direct Banking document, which sets out the basic principles for the secure use of direct banking, which may be amended by the Bank. The Bank publishes the Ten Security Principles on its website and they is also available at the Bank's points of sale. This document does not constitute a Notice within the meaning of the GTC.

"eIDAS" is 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, as amended, regulating, in particular, electronic signatures and electronic identity.

5 Act No. 370/2017 Coll., on payment systems, as amended

"**Electronic signature**" is an electronic signature within the meaning of eIDAS, based, in particular, on the Methods provided to you on the basis of the Agreement.

"**One-time Password**" is a security password sent via an SMS to the agreed mobile phone number, which serves as a one-time password to activate or unblock a Method or Mobilní banka, add or replace devices for KB Klíč or add a device for Mobilní banka, as well as in some cases to authorise transactions and to use the Security Password Method.

"**KB Klíč**" is a Method provided on the basis of the Agreement, based on the individual characteristics of the activated mobile application for the supported devices and knowledge of the security PIN code or biometrics, which makes it possible, in particular, to verify the signatory's identity, to sign documents electronically and to authorise payment transactions. This Method can be activated in various applications (e.g. in the KB Klíč application).

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

"**Client**" means the person who has entered into the Agreement with the Bank.

"**Client Hotline**" is a 24/7 telephone line with the number + 420 955 551 552 for calls in Czech and the number + 420 955 551 556 "Customer Service KB" for calls in English. In the event of a change of the telephone number, the up-to-date number is always available on the website.

"**Method**" is a means for your identification, authentication, authorisation and creation of Electronic Signature and, where applicable, KB Bank Identity, provided under the Agreement.

"**MojeBanka**" is an internet banking service that the Client may use on the basis of a direct banking agreement.

"**MůjProfil**" is a portal for the support and administration of Methods. MůjProfil is accessible to the Client on the Bank's website, where the Client logs in using any Method or, if enabled, directly from our internet banking.

"**National Point**" is a public administration information system supporting the process of electronic identification and authentication through a qualified system, administrated by the Digital Information Agency.

"**Business Day**" is a day other than Saturday, Sunday or public holiday within the meaning of the applicable regulations when the Bank is open for the provision of Banking Services and, simultaneously, when other institutions that participate in the provision of a Banking Service or on which the provision of a Banking Service is conditional are open for the provision of the relevant services.

"**Notices**" are communications setting out additional terms and technical aspects of the provision of Banking Services in accordance with the GTC and the applicable Product Terms and Conditions. The Certification Policy and the Ten Security Principles are not notices.

"**Chip Card PIN**" is a personal four-digit numerical identification number used to verify the authorisation to use the chip card.

"KB Klíč PIN" is a personal numeric code used to verify the authorisation for the application using the KB Klíč Method.

"**Payment Services**" mean Banking Services that are payment services within the meaning of the Payment Services Act (e.g., transfers of funds, issuance of payment instruments and cash withdrawals and deposits).

"**Terms and Conditions**" are these Terms and Conditions for Electronic Signature and KB Bank Identity, which represent the Product Terms and Conditions under the GTC.

"**Product Terms and Conditions**" are the Bank's terms and conditions governing the provision of individual Banking Services.

"**PUK**" is an eight-digit numeric code used to unlock the chip card.

"**QSCD**" (Qualified Signature Creation Device) is a type of hardware device that meets specific technical requirements, has been certified by a qualified trust services provider, and is used to create qualified electronic signatures within the meaning of the eIDAS Regulation.

"**List of Fees**" is a summary of all fees, other charges and other payments for Banking Services and acts related to Banking Services.

"**Agreement**" means the agreement under which the Client arranges the Method(s).

"**Private Key**" is the data for creating the Client's Electronic Signature in the form of a Certificate.

"**Technical Terms and Conditions**" is a document in which the Bank sets the technical parameters for the provision of direct banking services. The Bank publishes the Technical Terms and Conditions on its website. The Bank may change the Technical Terms and Conditions. Technical Terms and Conditions do not constitute a Notice within the meaning of the GTC.

"**Public Key**" is the data for verifying the Client's Electronic Signature in the form of a Certificate.

The term "**GTC**" refers to our General Business Terms and Conditions.

10.2 Links to our website are links to the address www.mojebanka.cz or other internet addresses that we use or will use in connection with the provision of Banking Services.

Article 11. Final provisions

11.1 Where the terms “Electronic Signature Terms and Conditions” and “Electronic Signature Agreement” are used in agreements and other documents concluded between us and you or in contractual documents forming an integral part of such agreements, they mean the Electronic Signature and KB Bank Identity Terms and Conditions and the Electronic Signature and KB Bank Identity Agreement, respectively.

11.2 We may change the Terms and Conditions from time to time in the manner set out in the GTC. We will inform you of any such change via the relevant direct banking service or in the manner specified in the GTC.

11.3. These Terms and Conditions repeal and replace the Electronic Signature Terms and Conditions of 16 April 2024.

11.4 The Terms and Conditions enter into effect on 1 May 2026.