TERMS AND CONDITIONS FOR THE PROVISION OF ČSOB ELECTRONIC BANKING SERVICES

Československá obchodná banka, a.s., with its registered office at Žižkova 11, Bratislava 811 02, registered in the Companies Register of the Bratislava III Municipal Court, Section Sa, File No. 4314/B, ID No.: 36 854 140 (hereinafter referred to as the "**Bank**"), issues these Terms and Conditions for the Provision of ČSOB Electronic Banking Services (hereinafter referred to as the "**ELB Terms and Conditions/Terms and Conditions**"). The ELB Terms and Conditions govern the legal relationships between the Bank and its Clients in connection with the provision of selected Products and Services via means of distance communication in accordance with Act No. 492/2009 Coll. on Payment Services (and amending certain laws) as amended (hereinafter referred to as the "**Payment Services Act**"), and the current General Business Terms and Conditions (hereinafter referred to as the "**GBTC**"). Legal relationships between the Bank and its Clients are governed by the laws of the Slovak Republic.

Article 1

Basic Terms

1. **Apps and Application Program Interface** through which Services are provided on the ČSOB Platform:

   a) Web app (hereinafter referred to as the "**Moja ČSOB App**");

   b) Mobile app (hereinafter referred to as the "**ČSOB SmartBanking App**");

   c) Application Program Interface ČSOB API, PSD2 (hereinafter referred to as the "**ČSOB API**");

   d) ČSOB SmartToken App.

2. **ČSOB SmartBanking App** is a mobile application that Clients can install on their own devices (e.g., smartphones, tablets) from official digital distribution platforms such as Google Play, the App Store, and Huawei AppGallery, thereby gaining access to the part of the Platform where ČSOB offers services of ČSOB Group Members and Partner Services.

3. **Moja ČSOB App** is a web app available on the ČSOB Website that allows Clients to use their Digital Identity to access the part of the Platform where ČSOB offers services of ČSOB Group Members.

4. **ČSOB SmartToken App** is an app that is used to (i) generate one-time codes for the Client's login, (ii) electronically sign payment orders sent via the Moja ČSOB App, (iii) activate the ČSOB SmartBanking App, and (iv) confirm online 3-D Secure payments.

5. **Authentication** is a process that enables the Bank to verify the Client's identity/Client's Digital Identity or their authorisation to use a means of payment, including the use of personalised security features.

6. **Authorisation** is a legal act by which the Client expresses consent to the execution of a payment transaction using Security Features.

7. **Secure Contact** is a mobile phone number and email address that the Client specifies in advance in the Agreement or in the Agreement on the Activation of Electronic Banking Services. The Bank uses this contact information to send messages regarding the security of electronic banking.

8. **Security Feature** is a component of Digital Identity and a means of enhancing the security and confidentiality of distance communication via the ELB Service between the Client and the Bank, primarily ensuring Client Authentication and Client Authorisation.

9. **ČSOB/ČSOB Group Members or individually a ČSOB Group Member** for the purposes of these ELB Terms and Conditions, this includes the Bank, ČSOB Poisťovňa, a.s., with its registered office at Žižkova 11, Bratislava 811 02, registered in the Companies Register of the Bratislava III Municipal Court, Section Sa, File No. 444/B, ID No.: 31 325 416, and ČSOB Leasing, a.s., with its registered office at Žižkova 11, Bratislava 811 02, registered in the Companies Register of the Bratislava III Municipal Court, Section Sa, File No. 1220/B, ID No.: 35 704 713.

10. **Identification Number/IPPID** is a unique and non-transferable number assigned by ČSOB to the Client upon the conclusion of the Client Agreement or upon the conclusion of the Agreement on the Activation of Electronic Banking Services.

11. **Client Agreement** is an agreement on the basis of which a consumer becomes a ČSOB Client and obtains a Digital Identity and access to the ČSOB Platform, through which they can use the available Services. The terms "**Digital Identity**" and **"ČSOB Digital Platform" (ČSOB Platform/Platform)** are defined in the Terms and Conditions for ČSOB Digital Identity.

12. **Means of Distance Communication** is a means that can be used to provide financial services remotely without the Bank and the Client being physically present at the same time.

13. **Product Agreement** is a financial service agreement concluded remotely between a ČSOB Group Member and the Client for selected Products/Financial Services via a Means of Distance Communication**.**

14. **Payment Account** is a current account or another type of account as defined by the Payment Services Act.

15. **Services** are services of the ČSOB Group Members and Partner Services, which include:

    a) ČSOB Financial Services/Products which the Client obtains by entering into a Product Agreement with a ČSOB Group Member:

        (i) Banking financial services;
        (ii) Insurance financial services;
        (iii) Lease financial services;

    b) SmartSlužby+;

    c) Kate—proactive personalised services with added value and

    d) Personalised services—personalised Partner Services (in cooperation with ČSOB partners) or ČSOB Group Members, within the scope specified in the Personalised Marketing Agreement:

        (i) Personalised marketing messages;
        (ii) Kate Coin.

    The description of the selected Services in paragraph 15(b), (c), and (d) of this Article is further specified in the Terms and Conditions for ČSOB Digital Identity. The scope of Services may vary by App.

16. **ČSOB Electronic Banking Service** (hereinafter referred to as the "**ELB Service**" or "**ELB Services**") is a service provided by the Bank through which the Client gains access to a selected Service or Product, with the option to enter into a Product Agreement or other types of agreements.

17. **Partner Services** are services provided by suppliers of goods or services with whom ČSOB collaborates; the Client is also entitled to obtain these goods or services through the SmartSlužby+ service. The current list of Partner Services, as well as the technical specifications for their provision, are available on the ČSOB Website, which ČSOB updates on an ongoing basis.

18. **Durable Medium (Agreements and Documents)** is a separate section/tab (electronic mailbox or folder) within the ČSOB Platform designed for the delivery and storage of contractual documentation and other documents related to the contractual relationship between ČSOB and the Client.

19. **Account** is an account established and maintained in accordance with generally applicable laws under a Product Agreement, specifically a current account, a deposit account, or a savings account.

20. **Website/ČSOB Website** is www.csob.sk.

21. **Agreement** is a Client Agreement or an Agreement on the Provision of the ELB Service**.**

22. **Agreement on the Provision of the ELB Service** is an agreement entered into between the Bank and the Client regarding the provision of the ELB Service. For the purposes of these ELB Terms and Conditions, the Agreement on the Provision of an ELB Service means an Agreement on the Provision of the ČSOB Electronic Banking Service together with the Agreement on the Activation of ČSOB Electronic Banking Services, including the Power of Attorney for managing the funds in the account.

23. **Distance Agreement** is an agreement between ČSOB and the Client regarding the provision of a financial service, which is negotiated and concluded exclusively through one or more means of distance communication.

24. **Legal Representative of the Minor** is a representative of a minor under applicable law.

Article 2

General Provisions

1. ELB Services are provided under the Agreement and through the Apps, using Means of Distance Communication. The Bank provides the ELB Service on a contractual basis in accordance with the laws applicable in the Slovak Republic.

2. The ELB Service shall be without prejudice to the terms and conditions and the content of the Product Agreement and the relevant business terms of business, as well as the rights and obligations arising therefrom. The use of ELB Services is equivalent to written communication.

3. ELB Services are provided in Slovak. The Bank is authorised to provide selected ELB Services or their individual features in English as well.

4. The Bank notifies the Client via the ELB Services of the balances in the Accounts and of completed transactions. The Client is required to preliminarily verify whether the settlement statements correspond to the payment orders submitted and whether the submitted payment orders were executed or refused by the Bank. The Client is obliged to notify the Bank without undue delay of any errors found in the settlement or other discrepancies.

5. Information and documents sent by the Bank to the Client via the ELB Services are deemed to have been delivered on the date they were made available on a durable medium of the relevant App and became available to the Client.

6. To ensure the smooth use of the ELB Services, the Bank requires a mobile device running the Apple iOS or Google Android operating system with online access.

Article 3

Client and Client Authentication

1. For the purposes of these ELB Terms and Conditions, “Client” means:

   a) A natural person who has become a client under the Client Agreement;

   b) Account Holder—a natural person who has an account with the Bank;

   c) Authorised Person—a natural person authorised by the Account Holder to use the ELB Services and to manage funds in the Account Holder’s designated accounts via the ELB Services, or the holder of a payment card issued for the Account Holder’s account. The Authorised Person also has access to all information regarding the Account Holder’s accounts that is provided by the relevant ELB Service and is subject to bank secrecy. For the purposes of these ELB Terms and Conditions, the term “Authorised Person” also includes the Account Holder—a natural person. For accounts held by Account Holders under the age of 18, only the Legal Representative of the Minor or the minor Account Holder may be designated as the Authorised Person.

2. The Client is authenticated in:

   a) Moja ČSOB App using their Identification Number (IPPID) and the PIN for their IPPID. Authorisation is carried out via a one-time code generated by the relevant Authorisation Device. For Authentication and Authorisation, the Bank is not required to request a one-time code generated by the relevant authorisation device for every transaction;

   b) ČSOB SmartBanking App using their Identification Number (IPPID) and the PIN for their IPPID. Before first authentication, the ČSOB SmartBanking App must be installed on a mobile device. Each Client's authorisation contains an Identification Number (IPPID) and is authenticated by entering the PIN for the IPPID. The Identification Number (IPPID) is stored in encrypted form in the app and does not need to be re-entered.

3. The Bank shall block the Client's Identification Number (IPPID) or the use of the ČSOB Smart Token App, thereby preventing the Client from accessing ELB Services, if incorrect authentication, authorisation, or activation data is entered repeatedly, to the extent specified in the Technical Parameters and Specifications for the Operation of Electronic Banking Services (hereinafter referred to as the "**Service Specification**"), which is published on the ČSOB Website under the Important Documents tab.

   The Client may request that their access or Authentication/Authorisation Code be unblocked in person at a branch or by phone, provided they can authenticate themselves. The Bank shall refuse the Client's telephone request if it processed the Client's most recent request to unblock the Identification Number (IPPID) or Authentication/Authorisation Code on the day (D) or the preceding business day (D-1) following the Client's current telephone request for unblocking.

Article 4

Security Features and Protection of ELB Services

1. Security Features include:

   a) PIN (for the Identification Number) is a numeric code used for the Client's Authentication. The Bank may allow the Client (on mobile devices with biometric functionality supported by the Bank in the SmartBanking App) to replace the PIN with another Security Feature (such as biometric data). The PIN can only be changed by the Client themselves, in the self-service area accessible before logging into the Moja ČSOB app, or in the SmartBanking App. In order to successfully change the PIN, the Client must have provided the Bank with Secure Contacts: (i) a mobile phone number and (ii) an email address.

   b) Authentication/Authorisation Code is a one-time numeric code with a limited validity period used for the Client's Authentication or Authorisation with the Bank, which is either:

   (i) A code generated using the ČSOB SmartToken App;
   (ii) A numeric OTP code (one-time password, a single-use numeric security code) sent by the bank to Secure Contacts. The OTP code is generated separately for each Authentication, or
   (iii) numeric code (SMS key) sent by the bank to a predefined mobile phone number (hereinafter referred to as the "**Secure Phone Number**"). An SMS key is generated separately for each Authentication/Authorisation.

   c) Password for the ČSOB SmartToken App is a numeric code that the Client selects when activating the ČSOB SmartToken App and enters each time they use it.

   d) Activation Code is a one-time code used to confirm the activation process for the ČSOB SmartBanking App and the ČSOB SmartToken App.

2. Once the Security Features have been assigned, the Client is required to take all reasonable measures to ensure their protection. The following are considered reasonable measures:

   a) Prevent any disclosure or access of Security Features to or by other persons;

b) Not to write down the PIN (for the Identification Number) or passwords, and not to disclose them to any third party (including Bank employees);

c) Use a properly licensed antivirus and anti-spyware program with the latest updates;

d) Not to use public or unknown networks;

e) After finishing work with the ELB service, it is necessary to log out properly.

3. The Bank reserves the right to decide on the use of the Client's strong authentication elements (i.e., at least two-factor authentication, SCA—Strong Customer Authentication), namely the IPPID, PIN, and Authentication Code generated by the relevant authorisation and authentication device that the Client currently has assigned and activated for the ELB Services.

4. ELB Services are provided via public communication networks. The Bank is not responsible for their security and therefore cannot influence the outcome if the Client suffers damage as a result of the misuse of transmitted messages due to unauthorised actions by third parties.

5. SMS messages and email notifications are not digitally signed or encrypted.

6. Given the specific nature of ELB Services, the Bank has the right to archive individual Client orders placed by telephone or via online requests in the form of audio recordings, copies of sent SMS messages, or copies of online requests. Audio recordings, SMS messages, and records of online requests are securely archived in electronic form at the Bank. The conditions and time limits for archiving are governed by generally applicable laws, in particular Act No. 483/2001 Coll. on Banks and on the supplementation of certain acts as amended. The Bank archives data in a manner that allows for the retrieval of transactions and the correction of errors.

7. The records listed above may be used to protect the Bank's legitimate interests as evidence in any proceedings before courts or other authorities.

Article 5

Apps and Application Program Interface

1. Moja ČSOB App

1.1. The Moja ČSOB app enables secure distance communication between the Client and the Bank/ČSOB. Its purpose is to provide selected Services and ELB Services within the Platform's digital environment.

1.2. The components of Digital Identity used to log in to the Moja ČSOB App are: Identification Number (IPPID) and PIN (for the Identification Number). The Bank may require users to log in using three elements of their Digital Identity: Identification Number (IPPID), PIN (for the Identification Number), and Authentication/Authorisation Code.

2. ČSOB SmartBanking App

2.1. The ČSOB SmartBanking App facilitates secure distance communication between the Client and the Bank/ČSOB. Its purpose is to provide selected Services/ELB Services within the Platform's digital environment.

2.2. The ČSOB SmartBanking App is automatically set up/activated upon setting up the Moja ČSOB App. An Authorised Person has access to the Account Holder's accounts and to selected ELB Services and related information.

2.3. To activate the ČSOB SmartBanking App, it is necessary to enter the Identification Number, PIN (for the Identification Number), and Activation Code. The ČSOB SmartBanking App can be deactivated in the "Settings" menu, or via a phone request (at +421 2 5966 8844), or by uninstalling the ČSOB SmartBanking App from the mobile device.

2.4. Each subsequent action by the Client includes an Identification Number and is authorised by entering a PIN (for

the Identification Number). The Identification Number is stored in encrypted form in the ČSOB SmartBanking App and it is not necessary to re-enter it.

2.5. The Client is required to comply with the Bank's security guidelines for using the ČSOB SmartBanking App, as set forth in the SmartBanking - ČSOB section under "Device Protection," and in particular, not to make any unauthorised modifications to the mobile device's operating system.

2.6. The Client is obliged to use only mobile devices on which no jailbreak or root modifications have been made to operate the ČSOB SmartBanking App and the ČSOB SmartToken App; furthermore, the Client must not use software or other modifications that interfere with or block the detection of jailbreak/root on the mobile device.

3. ČSOB API

3.1. ČSOB API is an application program interface that provides access to payment initiation services (PIS), account information services (AIS—Account Information Service), and services confirming the availability of funds to execute a payment transaction linked to a payment card on a payment account (CPIIS—Card-Based Payment Instrument Issuer Service) in accordance with the Payment Services Act. It ensures the execution of payment orders issued by the Authorised Person—the user of the Account Holder's Payment Account—that were not entered into the Bank's information system, and provides the Authorised Person with access to the Account Holder's accounts and selected information. It is automatically set up upon installation of the Moja ČSOB App. A description of how to use the ČSOB API is provided in the document "ČSOB API (PSD2) Terms and Conditions" published on the ČSOB Website under the "Important Documents" tab.

3.2. The prerequisite for using the ČSOB API is:

a) Assigning the Authorised Person with the Identification Number, with access to the Moja ČSOB platform; and

b) granting the Authorised Person's consent to an Authorised Third Party and, at the same time, performing strong authentication of the Authorised Person within the ELB Services environment, where an Authorised Third Party is defined as a third party that has requested the Bank to facilitate the ČSOB API (PSD2), is listed in the register of the relevant national authority, and holds a qualified certificate within the meaning of the ČSOB API (PSD2) Terms and Conditions, and the Bank has permitted this person to mediate these ČSOB API (PSD2).

Article 6

Limits for the Client

1. Limits for the Client:

a) The main transaction limit is set by the Bank without restriction for the Account Holder, and for the Authorised Person, this limit is set by the Account Holder in the power of attorney for the management of funds in the account;

b) The limits on the Authentication/Authorisation Code are set by the Bank and specified in the Service Specification document.

2. **The functionality of ELB Services for** minor Account Holders (excluding accounts held without Legal Representatives of Minors) applies to special accounts subject to the following terms and conditions:

a) As for accounts held by an Account Holder under the age of 15, the Account Holder may only have passive access, while the Legal Representative of the Minor may have active access; the main transaction limit for the account is set by the Legal Representative of the Minor;

b) As for accounts held by an Account aged 15 to 18, the Account Holder may have active access; the main transaction limit for the account is set by the Legal Representative of the Minor;

c) An Account Holder under the age of 18 may only manage their own account electronically and use the available ELB Services in connection with their own account;

d) Upon the Account Holder reaching the age of 18, or if a minor (aged 16 or older) attains legal age as a result of marriage, their access to ELB Services shall not terminate upon proof of this fact, unless otherwise agreed with the Bank. As of that date, the authorisation of the Legal Representative of the Minor as an Authorised Person to manage funds in this Account Holder's Accounts in relation to ELB Services shall cease.

3. The Account Holder automatically has visibility into all of their own products in the ELB Services after logging in with any of the IPPIDs issued to them. The Account Holder automatically has an unlimited transaction limit set on their own accounts. The Account Holder is authorised to set the main transaction limit on the account (the so-called per-transaction limit) for each Authorised Person whom they have authorised to manage funds in their accounts through the ELB Services. If an Authorised Person who is not the Account Holder requests that a daily/weekly limit be set for an authorisation device or a limit for an individual transaction submitted to the Bank in an amount higher than the main transaction limit on the account set by the Account Holder, the main transaction limit on the account set by the Account Holder shall be binding on the Bank.

Article 7

Client's Rights, Obligations and Responsibility

1. The Client is required to use the ELB Services and familiarize themselves with the Service Specifications, comply with the procedures set forth therein, and take all necessary measures to protect them, in particular ensuring that no other person becomes aware of the Security Features in use; the Client must not disclose or reveal these Security Features to any other person, nor record them in any easily recognisable form, nor store or carry them together with the Means of Distance Communication for the ELB Services. If the account is held in the name of the Legal Representative of the Minor, the Legal Representative of the Minor is responsible for protecting the Security Features.

2. If the Client:

   a) Forgets their Security Features, they are required to set up new Security Features or visit a Bank branch, where new Security Features can be set up.

   b) Discovers that the Security Features/Means of Distance Communication for ELB Services (e.g., a mobile phone/mobile device, etc.), or discovers that an unauthorised person is aware of their Security Features, they are required to report this fact immediately to the Bank in person at a Bank branch or by phone at +421 2 5966 8844 and request that they be blocked. Upon receiving this notification and the Client's request, the Bank shall immediately block the Client's access to the ELB Services and agree on the next steps with the Client. In the case of a telephone notification, for technical reasons the Bank does not provide the Client with proof that access to the ELB Services has been blocked; however, this telephone conversation is recorded for the purpose of verifying the time the incident was reported and its content. The Bank shall take all reasonable measures to prevent further use of the ELB Services, even if the Client has acted with gross negligence or fraudulently. The Client is required to cooperate fully with the Bank in implementing any remedial measures proposed by the Bank. If the Client fails to accept the proposed measures necessary to avert imminent damage, the Bank shall not be liable for any damage incurred by the Client as a result.

   c) Discovers a transaction that was not executed based on their instruction/order, an error, or any other discrepancy in the management of the account for which ELB Services are provided, the Client is required to notify the Bank in person at a Bank branch or by telephone.

3. The Client shall bear any loss up to EUR 50 resulting from any unauthorised payment transactions caused by the use of a stolen or lost payment instrument or the misuse of such a payment instrument by an unauthorised person due to the Client's negligence in protecting the Security Features. However, the Client shall bear all losses related to unauthorised payment transactions if they were caused by the Client's fraudulent conduct, intentional failure to fulfil one or more

obligations under these Terms and Conditions (in particular those governing the use of the ELB Service or ensuring the protection of Security Features after their assignment) as a result of the Client's gross negligence.

4. The Client shall not be liable for any financial losses resulting from the use of a stolen, lost, or misused means of payment:

   a) After the moment of delivery of the notification pursuant to Article 7(2)(b) of these Terms and Conditions, except in cases where the Client acted fraudulently;

   b) If the theft, loss, or misuse could not have been detected by the Client prior to the execution of the payment transaction, except in cases where the Client acted fraudulently;

   c) If such losses were caused by the acts or omissions of a Bank employee or a person authorised to perform activities on behalf of the Bank;

   d) If the Bank does not require strong payer authentication or if the Bank applies an exemption from strong payer authentication, except in cases where the Client acted fraudulently.

5. In the case of a payment order by the Account Holder to top up credit for mobile operators, even if there are insufficient funds in the Account Holder's account during the period between the submission of the order and the actual debiting of the amount from the Account Holder's account, and this constitutes an unauthorised overdraft of funds in the Account Holder's account, to which the Bank's rights apply pursuant to the Terms and Conditions for Current Accounts and the Bank's applicable Price List (hereinafter referred to as the "**Bank's Price List**"), the Bank is entitled to debit the amount for the credit top-up from the Account Holder's account.

6. Output information (confirmation of the Bank's receipt of a payment order, notifications) regarding instructions shall be provided in accordance with the Client's requirements to the address specified by the Client, using the contact details set forth in the Agreement, which the Client may unilaterally change through selected ELB Services.

Article 8

Bank's Rights, Obligations and Responsibility

1. The Bank provides the selected means of communication for ELB Services and Security Features for ELB Services only to the relevant Client. The Bank is obliged to perform Client Authentication before granting access to the ELB Services.

2. Upon notification of the facts pursuant to Article 7(2) of these Terms and Conditions, the Bank shall take all necessary measures to suspend further use of the ELB Services, even if the Client has acted with gross negligence or fraudulently.

3. The Bank shall be liable for:

   a) The failure to execute a transaction or the incorrect execution of a transaction that the Client is entitled to have executed;

   b) Transactions carried out without the Client's authorisation. The Bank shall not be liable if the Client acts in violation of the provisions of these Terms and Conditions, in particular in violation of the Client's obligations under Article 7(2) and (3).

4. In the cases specified in Article 8(3), the Bank shall proceed in accordance with the currently applicable Terms and Conditions for Current Accounts.

5. The provision of Article 8(3) shall not apply if the Bank demonstrates that the Client has violated its obligations set forth in these Terms and Conditions.

6. Within the ČSOB Platform, the Bank accepts only data transmitted via distance communication that is complete, conforms to the prescribed formats, and has been authenticated in accordance with the selected App. The Bank is entitled to refrain from executing or to refuse to execute transactions in other cases that prevent the execution of the transaction pursuant to these ELB Terms and Conditions or other contractually agreed terms and conditions relating to the provision of other services or products of the Bank, in the event of insufficient funds in the Account Holder's accounts from which the transactions are to be debited, as well as in the event that the Account Holder's accounts are frozen.

7. The Bank shall not be liable for any damage resulting from incorrectly submitted or double-entered payment orders (transactions) or for the non-execution of incomplete or unauthenticated transactions submitted to the Bank via the ELB Services, unless such damage was caused by the Bank's fault.

8. The Bank is entitled to charge fees for the use of ELB Services in accordance with the Bank's current Price List. Fees for sending "Payment Card Transaction" information are charged to the Account Holder's account to which the payment card is issued. When applying fees, the section of the Bank's Price List that applies to the specific account type shall be used. The Bank's current Price List is available at the Bank's premises, which are open to the public, and on the Bank's Website.

9. The types of interest rates that may apply to individual Services are listed in the relevant Interest Rates document. Current documents and Interest Rates are available at all Bank branches and on the ČSOB Website.

10. The Bank is entitled to block the Client's access to the ELB Services:

    a) For reasons related to the security of the ELB Service or the means of payment;

    b) For reasons of suspected non-authenticated or fraudulent use of the ELB Service or the means of payment; or

    c) If such an obligation arises for the Bank from a generally binding legal regulation. The Bank shall notify the Client of the blocking of the ELB Service for this reason and of the next steps as soon as possible. If, in the event that the use of the Identification Number (IPPID) is blocked, the relevant Client wishes to continue using ELB Services, they are required to visit any branch of the Bank in person and provide written consent to the change of the Identification Number (IPPID). If the Bank determines that the blocking of the use of the Identification Number (IPPID) is unjustified and not necessary to protect the Client's rights when using the ELB Services, it has the right to unilaterally lift the existing block on the Client's access to the provided ELB Services, even without the Client's consent.

    d) If the Client's identity cannot be fully verified due to the data subject's withdrawal of consent to the processing of biometric data.

11. The Bank reserves the right to suspend the provision of ELB Services, including payment services. In cases where such an interruption in the provision of ELB Services can be scheduled, the Bank shall provide appropriate notice of such a scheduled interruption of ELB Services.

Article 9

Cut-Off Times

1. The Bank accepts Clients' instructions via ELB Services 24 hours a day, 7 days a week, or 365 days a year.

2. The time limits for submitting payment orders electronically and the cut-off times are specified in the document "Cut-Off Times for Payment Transactions" (hereinafter referred to as the "Cut-Off Times"), which is available to the public at the Bank's business premises and on the ČSOB Website.

3. The Client is not entitled to revoke a payment order on the due date. A SEPA payment order with a future due date sent via ELB Services may be revoked via selected ELB Services no later than the day before its due date, in accordance with the provisions of the Cut-Off Times document. A SEPA payment order can be revoked:

    a) By selecting "Cancel" in the "Account Transactions" section under "Pending Payments" in the Moja ČSOB App;

    b) by selecting "Cancel Payment" in the "Account Transactions" section under "Pending Payments" in the ČSOB SmartBanking App.

Article 10

Final Provisions

1. The Bank processes personal data for the purpose of providing ELB Services in accordance with these Terms and Conditions. Information regarding the processing of personal data is specifically outlined in the document Privacy Policy for ČSOB Mobile Apps and generally in the document Privacy Policy. Both documents should be read together.
2. The submission and handling of Client's complaints and claims regarding the accuracy and quality of the provision of ELB Services are governed by the Bank's Complaints Procedure, which is published in the Bank's premises available to the public and on the ČSOB Website.
3. The Account Holder is notified of transactions carried out on the account via a paper account statement or, upon agreement between the Bank and the Account Holder, in electronic form as a record on a Durable Medium.
4. In light of technical and business developments, the Bank is entitled to unilaterally modify the scope of ELB Services, add new applications and features, and discontinue inactive apps or modify their functionality. The Bank is entitled, in order to ensure the highest level of security for ELB Services, to discontinue the use of Security Features or modify their settings if, due to causes beyond the Bank's control, there is a risk of a decline in their security level, provided that the Client is notified in advance. The change is possible even without the Bank stating the reason for the change. The Bank shall notify the Client of any changes to the Terms and Conditions and their effective date by publishing information regarding changes to the scope of ELB Services on the ČSOB Website, by publishing these documents in the Bank's premises available to the public, and by notifying the Client no later than two months prior to the effective date of the relevant change. If the Client objects to such a change and no agreement is reached, the Client is entitled to terminate their contractual relationship with the Bank with immediate effect, without incurring any related fees. This right must be exercised before the proposed effective date of these changes. Information included in an Account statement is also considered written notification to the Client.
5. The mailing address for sending documents to the Bank is: Československá obchodná Banka, a.s., Žižkova 11, 811 02 Bratislava. The mailing address for sending documents to the Account Holder is the mailing address designated by the Account Holder, and the mailing address for sending documents to the Authorised Person is the mailing address designated by the Authorised Person. The Account Holder and the Authorised Person are required to notify the Bank in writing of any change in their mailing address, contact telephone number, or email address.
6. The mutual rights and obligations of the Bank and the Client not provided for in the Agreements or these ELB Terms and Conditions shall be governed by the GBTC.
7. These ELB Terms and Conditions replace the Terms and Conditions for the Provision of ČSOB Electronic Banking Services valid from 1 February 2026 in their entirety.
8. The Terms and Conditions shall enter into force on 1 July 2026.