# Obchodné podmienky pre elektronickú správu účtov

vedených bankou **Fio banka, a.s.**, IČO: 61858374, V Celnici 1028/10, 117 21 Praha 1, Česká republika, zapísanou v obchodnom registri vedenom Mestským súdom v Prahe, oddiel B, vložka 2704, prostredníctvom organizačnej zložky **Fio banka, a.s., pobočka zahraničnej banky**, IČO: 36869376, Dunajská 1, 811 08 Bratislava, zapísanej v obchodnom registri vedenom Okresným súdom Bratislava I, oddiel: Po, vložka č.: 1875/B (ďalej aj len „Banka“)

## Čl. I. Predmet úpravy

1. Banka umožňuje svojim klientom na základe zmluvy o elektronickej správe účtov (ďalej len „zmluva“) elektronicky spravovať ich účty vedené Bankou, prípadne priamo bankou Fio banka, a.s., IČO: 61858374, ČR (ďalej tiež len „internetbanking“). Do internetbankingu sa oprávnená osoba prihlasuje za použitia svojho prihlasovacieho mena a prístupového hesla, prípadne i ďalšieho Bankou požadovaného údaja či bezpečnostného prvku (napr. SMS kódu či smartbankingu). Ak sa ďalej píše o internetbankingu, môže tým byť podľa povahy úpravy myslený taktiež tzv. „smartbanking“, teda služba priameho bankovníctva, pomocou ktorej Banka umožňuje svojim klientom na základe zmluvy elektronicky spravovať ich účty vedené Bankou, a to použitím na tento účel Bankou určenej aplikácie smartbanking v klientovom mobilnom zariadení. Pre smartbanking platia všetky nasledujúce ustanovenia rovnako ako pre internetbanking, ak nie je ďalej uvedené inak. Elektronickou správou účtov sa rozumie bezdokladové elektronické podávanie pokynov a využívanie ďalších služieb poskytovaných k účtu a získavanie informácií o účte a vykonaných službách. Oprávnenie na elektronickú správu účtu fyzickej osoby môže udeliť majiteľ účtu elektronicky v prospech tretej fyzickej osoby - klienta Banky určením jeho prihlasovacieho mena a prideleného identifikačného čísla klienta. Oprávnenie na elektronickú správu účtu právnickej osoby môže udeliť písomne v prospech tretej fyzickej osoby osoba oprávnená konať za právnickú osobu. Pri udelení plnomocenstva určí majiteľ účtu aj rozsah splnomocnenia, tzn. určí, ktoré úkony je splnomocnená osoba oprávnená vykonávať. Splnomocnenec používa spôsob autorizácie elektronickej komunikácie tak, ako ju má dohodnutú s Bankou.
2. Tieto obchodné podmienky pre elektronickú správu účtov (ďalej tiež len „Podmienky“ alebo „podmienky“) doplňujú alebo podrobnejšie upravujú niektoré ustanovenia zmluvy, prípadne k nim uvádzajú záväzný výklad. V prípade rozporu medzi úpravou v zmluve a Podmienkach platia ustanovenia zmluvy.
3. Vlastnoručným podpisom sa rozumie podpis urobený vlastnou rukou príslušnej osoby (klienta, oprávnenej osoby atď.) na listine (napr. zmluva či iný listinný dokument) alebo biometrický podpis. Biometrickým podpisom sa rozumie podpis príslušnej osoby (klienta, oprávnenej osoby atď.) vyhotovený prostredníctvom špeciálneho zariadenia (napr. tablet, signpad), ktoré zachytáva nielen grafickú podobu podpisu, ale aj jeho dynamické prvky (napr. tlak, rýchlosť). Ak to Banka umožňuje, takým podpisom je možné podpisovať rôzne druhy dokumentov na pracoviskách Banky.

## Čl. II. Spôsob prenosu a zabezpečenia prenášaných dát

1. Všetky pokyny a informácie, ktoré sa dajú podať, resp. získať pomocou elektronickej správy účtov, sú prenášané medzi serverom Fio banky, a.s. a počítačom či obdobným mobilným zariadením, ako napríklad tzv. chytrým telefónom (smartphone) či tabletom, (ďalej aj len súhrnné označenie „zariadenie“ pre počítač, mobilný telefón, tablet a obdobné mobilné zariadenia) klienta prostredníctvom internetu. Prenášané dáta sú zabezpečené

prostredníctvom šifrovanej komunikácie (https) za pomoci certifikátu SSL serveru od spoločnosti GeoTrust Inc.

2. Klient je pred každým využitím služieb Banky poskytovaných prostredníctvom internetu (predovšetkým služby Internetbanking) a pred každým zadaním dôverných údajov do prihlasovacieho dialógu povinný najskôr overiť, či sú z jeho strany dodržané všetky povinnosti uložené v ods. 1 čl. XIII Podmienok. „Bezpečnostné opatrenia vo sfére vplyvu klienta, zabezpečenie zariadení klienta“. Banka nezodpovedá za škodu spôsobenú porušením tejto povinnosti. Ďalšie povinnosti klienta súvisiace s obmedzením rizík pri používaní služieb Banky prostredníctvom internetu, ako aj dôležité informácie a upozornenia na riziká, ktoré sa týkajú využívania služieb Banky prostredníctvom internetu, sú uvedené v čl. VIII. až XVa Podmienok.
3. Banka zriaďuje klientovi prístup na neverejné stránky servera Banky pomocou užívateľského mena a hesla, ktoré si klient zvolí a dohodnutým spôsobom odovzdá Banke. Klient je oprávnený heslo kedykoľvek zmeniť.

## Čl. III. Autorizácia elektronicky zadaných pokynov

1. Ak nie je ďalej uvedené inak elektronicky podané pokyny musia byť klientom autorizované pomocou bezpečnostného prvku, tzn. podpísané jedným z nižšie uvedených spôsobov alebo ich kombináciou, v závislosti od spôsobu zvoleného klientom, prípadne stanoveného Bankou (v takom prípade Banka nastaví v systéme defaultne jeden zo spôsobov autorizácie pokynov uvedených v tomto článku, pričom také nastavenie je klientovi prípadne umožnené zmeniť na iný Bankou akceptovaný spôsob autorizácie), a to podľa aktuálnych požiadaviek Banky na autorizáciu jednotlivých druhov pokynov (napr. podľa čl. VII Podmienok). Banka je oprávnená spôsoby autorizácie elektronicky podaných pokynov jednostranne meniť, t. j. je oprávnená požadovať autorizovanie pokynov aj spôsobom, ktorý nemusí byť popísaný v týchto podmienkach B. Pokyny podané elektronicky pomocou smartbankingu musia byť klientom autorizované zadaním PINu pre smartbanking, pričom tento spôsob autorizácie nie je možné kombinovať s ostatnými spôsobmi. Aplikácia smartbanking môže na niektorých mobilných zariadeniach umožniť nahradenie PINu pre smarbanking alebo prístupových údajov pre smartbanking použitím zabudovaného biometrického snímača. Ak to Banka umožňuje, klient je oprávnený pokyny podané prostredníctvom smartbankingu, autorizovať príslušným spôsobom autorizácie tiež prostredníctvom internetbankingu. Práva a povinnosti klienta podľa tohto čl. III. Podmienok sa obdobne použijú na osobu oprávnenú klientom k elektronickej správe jeho účtu, ak nie je výslovne uvedené inak. V súlade s predchádzajúcou vetou sa teda spôsob autorizácie (vrátane možnosti podávať pokyny bez autorizácie pomocou bezpečnostného prvku) môže pri jednotlivých osobách oprávnených nakladať zo zostatkom rovnakého účtu odlišovať, a klient ako majiteľ účtu už na nastavenie spôsobu autorizácie pokynov ďalších ním oprávnených osôb nemá vplyv.

1a Ak je Bankou a klientom (či osobou oprávnenou podávať či autorizovať pokyny za klienta) dohodnutý spôsob autorizácie elektronicky podávaných pokynov (prostredníctvom internetbankingu), rozumie sa tým stanovenie spôsobu autorizácie pokynov s využitím niektorého z Bankou využívaných bezpečnostných prvkov (napr. sms autorizačný kód, elektronický podpis či ich kombinácia), avšak iba vo vzťahu k tým pokynom, pri ktorých Banka autorizáciu s využitím niektorého bezpečnostného prvku vyžaduje; Banka je oprávnená pre niektoré druhy pokynov nevyžadovať autorizáciu s využitím bezpečnostného prvku, a to za podmienok stanovených v týchto Podmienkach (môže ísť o druhy pokynov, kedy pre takýto postup nie je potrebný špeciálny úkon zo strany klienta, i o druhy pokynov, kedy takýto postup musí klient najskôr autorizovať s využitím používaného bezpečnostného prvku). Ak to Banka umožňuje, klient je oprávnený elektronicky podané pokyny (napr. prostredníctvom internetbankingu, aplikácie tretích strán alebo tokenu pre službu API a pod.) autorizovať taktiež prostredníctvom zariadenia, na ktorom je zriadený prístup do smartbankingu (t. j. zariadenie, ktoré je spárované s internetovým bankovníctvom klienta); Banka je oprávnená klientovi

umožniť nastaviť si tiež dodatočnú autorizáciu PINom pre smartbanking alebo za použitia biometrického snímača.

1b **Elektronicky podané pokyny, ktoré nemusia byť klientom autorizované pomocou bezpečnostného prvku.** Za podmienok vymedzených v ods. 1c, 1d a 1e tohto čl. III. Podmienok a odo dňa, kedy Banka umožňuje alebo umožní takýto spôsob vykonávania elektronicky podaných pokynov, je klient oprávnený vykonať bez využitia bezpečnostného prvku nasledujúce typy elektronicky podaných pokynov:

- pokyn k prevodu z účtu klienta na iný účet tohto klienta vedený Bankou (ďalej aj len „prevod medzi účtami klienta“),
- pokyn k prevodu malej čiastky z účtu klienta (ďalej aj len „prevod malej čiastky“),
- pokyn k prevodu z účtu klienta na účet podľa preverenej šablóny (ďalej aj len „prevod podľa preverenej šablóny“).

Klient je oprávnený podať a autorizovať prostredníctvom internetového bankovníctva pokyn k povoleniu vykonávania jednotlivého typu prevodov bez autorizácie pomocou bezpečnostného prvku. Banka je oprávnená (nie však povinná) odo dňa, kedy umožní vyššie uvedené typy elektronicky podaných pokynov vykonávať bez autorizácie pomocou bezpečnostného prvku (t.j. odo dňa zahájenia takejto služby), automaticky povoliť klientovi vykonávanie jednotlivého typu takýchto prevodov i bez predchádzajúceho pokynu klienta k takémuto povoleniu. Klient je oprávnený podať prostredníctvom internetového bankovníctva pokyn (ktorý nie je autorizovaný pomocou bezpečnostného prvku) k zakázaniu vykonávania jednotlivého typu prevodu bez autorizácie pomocou bezpečnostného prvku. Ak klient zakázal uskutočňovanie prevodov bez autorizácie pomocou bezpečnostného prvku, musia byť takéto prevody klientom štandardne autorizované pomocou bezpečnostného prvku podľa ods. 1 tohto článku. I keď má klient povolené vykonávanie prevodov bez autorizácie pomocou bezpečnostného prvku, Banka je vždy oprávnená pri jednotlivom pokyne vyžadovať jeho autorizáciu pomocou bezpečnostného prvku.

1c **Prevod medzi účtami klienta.** Klient je oprávnený (za podmienok podľa ods. 1b. tohto článku) vykonať bez autorizácie pomocou bezpečnostného prvku elektronický pokyn k prevodu čiastky z účtu klienta na akýkoľvek iný účet tohto klienta vedený Bankou (majiteľom účtu platiteľa a účtu príjemcu musí byť teda rovnaká osoba).

1d **Prevod malej čiastky**. Klient je oprávnený (za podmienok podľa ods.1b. tohto článku) vykonať bez autorizácie pomocou bezpečnostného prvku elektronický pokyn malej čiastky z účtu klienta, a to do výšky limitov pre maximálnu výšku čiastky jednotlivého prevodu bez autorizácie pomocou bezpečnostného prvku. Banka je oprávnená stanoviť limit pre maximálnu výšku čiastky jednotlivého prevodu bez autorizácie pomocou bezpečnostného prvku až do 30 eur, limit pre maximálnu kumulatívnu výšku po sebe nasledujúcich prevodov bez autorizácie pomocou bezpečnostného prvku až do 100 eur od posledného pokynu autorizovaného pomocou bezpečnostného prvku a limit pre maximálny počet po sebe nasledujúcich prevodov bez autorizácie pomocou bezpečnostného prvku až do počtu šiestich prevodov od posledného pokynu autorizovaného pomocou bezpečnostného prvku; Banka je oprávnená nestanoviť limit pre maximálnu kumulatívnu výšku alebo limit pre maximálny počet. Ak je podaním elektronického pokynu prekročený akýkoľvek limit stanovený Bankou, takýto pokyn je klient povinný štandardne autorizovať pomocou bezpečnostného prvku podľa ods. 1 tohto článku. Elektronický podaný pokyn v inej mene než v EUR bude pre účely tohto ods. 1d prepočítaný aktuálnym kurzom Európskej centrálnej banky.

1e **Prevod podľa preverenej šablóny.** Klient je oprávnený (za podmienok podľa ods. 1b. tohto článku) vykonať bez autorizácie pomocou bezpečnostného prvku elektronický pokyn k prevodu čiastky podľa šablóny, ktorú klient označí v internetovom bankovníctve alebo, ak to Banka umožňuje, v smartbankingu za preverenú (pre účely týchto podmienok aj len „preverená šablóna“). Klient berie na vedomie a súhlasí, že sa bez autorizácie pomocou bezpečnostného prvku vykoná i elektronický pokyn, ktorý nebol zadaný s využitím preverenej šablóny, pokiaľ sa parametre tohto elektronického pokynu zhodujú so všetkými parametrami nastavenými

klientom v rámci preverenej šablóny, s výnimkou čiastky (preverená šablóna musí mať nastavený aspoň účet príjemcu, ostatné parametre sú nepovinné); ak je pri preverenej šablóne nastavená čiastka (tzn. mesačný limit), uplatní sa takýto limit i pre takto podávaný pokyn. Ak nie je v rámci preverenej šablóny nastavený účet platiteľa, platí, že preverenú šablónu je oprávnený použiť klient pre akýkoľvek účet, ktorý je oprávnený samostatne elektronicky spravovať, ak nestanoví Banka inak. Ak je v rámci preverenej šablóny nastavený účet platiteľa, platí, že preverenú šablónu je oprávnená použiť ktorákoľvek osoba, ktorá je oprávnená elektronicky spravovať účet platiteľa, ak Banka nestanoví inak. Klient je oprávnený stanoviť si v internetovom bankovníctve alebo, ak to Banka umožňuje, v smartbankingu mesačný limit pre vykonávanie takýchto prevodov bez autorizácie pomocou bezpečnostného prvku (mesačný limit sa nastavuje uvedením čiastky v rámci preverenej šablóny; ak mesačný limit nie je uvedený, platí, že preverená šablóna je nastavená s neobmedzeným mesačným limitom, ak nestanoví Banka inak). Ak je podaním elektronického pokynu prekročený tento limit, takýto pokyn je klient povinný štandardne autorizovať pomocou bezpečnostného prvku podľa ods. 1 tohto článku.

2. **Autorizácia elektronickým podpisom**. Banka dodá klientovi program, ktorý mu umožní vytvoriť si vlastný elektronický podpis – kľúč. Klient je oprávnený po začatí elektronickej komunikácie zmeniť kľúč. Zmenu kľúča uskutoční klient tak, že v programe dodanom Bankou si vytvorí nový kľúč, ktorého verejnú časť osobne poskytne Banke na jej pracovisku. V prípadoch, kedy Banka prostredníctvom internetbankingu vyzve klienta k zmene kľúča, je klient povinný túto zmenu uskutočniť v lehote uvedenej vo výzve. V opačnom prípade Banka kľúč po márnom uplynutí lehoty zruší. Po zrušení kľúča nebude klient môcť uskutočňovať pokyny, ktoré vyžadujú autorizáciu podľa čl. VII ods. 9 Podmienok, a to do doby, dokiaľ neuskutoční zmenu kľúča zhora uvedeným spôsobom. Verejnú časť svojho kľúča odovzdá klient osobne Banke pred spustením elektronickej komunikácie. Správa prístupu k tajnej časti kľúča a k heslu kľúča je plne v zodpovednosti klienta. Ak je klientom právnická osoba, musí každá fyzická osoba, ktorá je oprávnená v mene klienta podávať pokyny a získavať informácie, mať svoje užívateľské meno a heslo, ktoré je považované za užívateľské meno a heslo klienta, a svoj kľúč, ak si zvolila autorizáciu elektronickým podpisom. Manuál pre elektronickú aplikáciu Fio-podpis, určený pre inštaláciu a použitie elektronického podpisu, je možné získať na každej pobočke Banky alebo na webovej stránke Banky: http://www.fio.sk/spolocnost-fio/manualy-dokumenty-cenniky/manualy. Klient je povinný pri inštalácii a použití elektronického Fio-podpisu postupovať podľa uvedeného manuálu. Autorizáciu pokynu prostredníctvom elektronického Fio-podpisu vykonáva klient potvrdením pokynu (odkliknutím danej voľby) v elektronickej aplikácii Fio-podpis, pričom pred prvým potvrdením pokynu je potrebné uviesť svoje heslo k súkromnej časti kľúča do elektronickej aplikácie Fio-podpis. Klient má povinnosť odhlásiť sa z elektronickej aplikácie Fio-podpis vždy bezprostredne po ukončení práce s ňou a nikdy neponechávať mimo dohľadu svoje zariadenie, pokiaľ je klient prihlásený do elektronickej aplikácie Fio-podpis.
3. **Autorizácia jednorazovým sms kódom**. Klient oznámi Banke telefonické číslo, na ktoré bude Banka klientovi zasielať sms správy s jednorazovým autorizačným kódom. Autorizačný kód je určený vždy k jednoznačne definovanému pokynu (vrátane tzv. hromadného pokynu k viacerým transakciám, apod.). Klient si v rámci nastavenia podmienok autorizácie môže spomedzi možností ponúkaných Bankou zvoliť dĺžku autorizačného kódu (5 – 25 znakov), počet pokusov pre zadanie kódu (1 – 5 pokusov) a platnosť autorizačného kódu (max. 20 minút). V prípade prepadnutia platnosti autorizačného kódu (vygenerovania nového autorizačného kódu k zadanému pokynu, uplynutiu stanovenej doby platnosti) klient môže požiadať o zaslanie nového jednorazového autorizačného kódu. Autorizáciu pokynu prostredníctvom sms kódu vykonáva klient uvedením zaslaného sms kódu do príslušného poľa formulára pre zadávanie pokynov v rámci internetbankingu po tom, čo sa riadne prihlásil do internetbankingu. Ak je klientom vložený sms kód zhodný s sms kódom vygenerovaným a zaslaným Bankou, je pokyn autorizovaný. Banka je oprávnená z bezpečnostných dôvodov

zrušiť zasielanie sms správ s jednorazovým autorizačným kódom na telefónne číslo oznámené klientom v prípade, že vznikne podozrenie, že telefónne číslo nie je vo výhradnej dispozícii klienta; v takom prípade je možné nové autorizačné číslo nastaviť osobne na pobočke Banky.

3a. **Autorizácia PINom pre smartbanking.** Pre používanie smartbankingu si klient do svojho mobilného zariadenia opatrí Bankou určenú aplikáciu smartbanking umožňujúcu poskytovanie tejto služby podľa operačného systému mobilného zariadenia (na internetových stránkach Banky je možné nájsť odkazy na autorizované zdroje tejto aplikácie). Bankou určenými aplikáciami smartbanking nemusia byť podporované všetky typy mobilných zariadení a ich operačné systémy. Klient zriadi prístup do smartbankingu prostredníctvom QR kódu, konkrétne nasledujúcim spôsobom: i) klient zadá (a autorizuje) pokyn v internetbankingu pre vygenerovanie QR kódu (jednorazový kód s obmedzenou platnosťou); tento pokyn musí byť riadne autorizovaný elektronickým podpisom a / alebo jednorazovým sms kódom v závislosti od spôsobu autorizácie zvolenej klientom, ii) klient použije vygenerovaný QR kód alebo číselný kód v smartbankingu pre spárovanie zariadení, iii) klient si vo smartbankingu zriadi prístupové heslo do smartbankingu a prípadne tiež PIN pre autorizáciu pokynov prostredníctvom smartbankingu. Autorizáciu pokynu prostredníctvom PINu pre smartbanking vykonáva klient zadaním PINu pre smartbanking do príslušného poľa pre zadávanie pokynov na zariadení, na ktorom je zriadený prístup do smartbankingu (t. j. zariadenie, ktoré je spárované s internetovým bankovníctvom klienta).

3b. **Autorizácia za použitia biometrického snímača.** Pokiaľ je už nastavený spôsob autorizácie podľa ods. 3a, na vybraných mobilných zariadeniach môže aplikácia smartbanking umožniť nahradenie PINu pre smartbanking alebo prístupových údajov pre smartbanking použitím zabudovaného biometrického snímača. Banka je oprávnená požadovať autorizáciu PINom pre smartbanking aj v prípade, ak má klient zvolenú autorizáciu za použitia biometrického snímača. Možnosť použitia biometrického snímača klient nastaví v aplikácii smartbanking a jeho nastavenie autorizuje PINom pre smartbanking. Pred nastavením použitia biometrického snímača banka odporúča klientovi zoznámiť sa s princípmi jeho fungovania v použitom mobilnom zariadení. Banka nezodpovedá za správne fungovanie biometrického snímača a klient nastavením jeho použitia pre smartbanking na seba preberá riziko vyplývajúce z možných chýb spojených s jeho fungovaním. Aplikácia smartbanking ani iné systémy banky nezískavajú, nespracovávajú ani neukladajú žiadne biometrické dáta klienta. Zrušenie možnosti použitia biometrického snímača sa nastavuje potvrdením príslušnej voľby v smartbankingu. Pre alternatívnu autorizáciu pomocou passcode (ak Banka umožňuje takýto spôsob autorizácie) do telefónu platia rovnaké pravidlá a povinnosti ako pre autorizáciu pomocou biometrického snímača.

4. Nastavenie spôsobu a podmienok autorizácie podľa ods. 2 a 3 konkrétneho klienta je uvedené v Zmluve, prípadne v Protokole o nastavení autorizácie elektronických pokynov. Nastavenie spôsobu a podmienok autorizácie PINom pre smartbanking podľa ods. 3a a prípadné následné nastavenie autorizácie použitím biometrického snímača podľa ods. 3b je považované za nastavenú autorizáciu elektronických pokynov podľa Zmluvy o elektronickej správe účtov okamžikom zriadenia smartbankingu klientom podľa postupu uvedeného v odseku 3a tohto článku (resp. okamihom nastavenia použitia biometrického snímača podľa ods. 3b), i keď tento spôsob autorizácie nie je uvedený v Zmluve či v Protokole o nastavení autorizácie elektronických pokynov.

5. Spôsob a podmienky autorizácie podľa ods. 2 a 3 môže klient meniť osobne na pobočke Banky. Spôsob a podmienky autorizácie podľa ods. 1c až 1e a ods. 3a môže klient meniť elektronicky prostredníctvom internetového rozhrania internetbankingu, ak Banka nestanoví inak. Spôsob a podmienky autorizácie podľa ods. 3a (ak to Banka umožňuje) a ods. 3b môže klient zmeniť elektronicky prostredníctvom aplikácie smartbanking.

## Čl. IV. Zriaďovanie a rušenie podúčtov bežného účtu a rušenie účtov pomocou elektronickej správy

1. Prostredníctvom elektronickej správy účtov sa dajú zriaďovať a rušiť podúčty bežného účtu (ďalej len podúčty), ak to je výslovne uvedené ako jedna z možností v čl. VII. podmienkou pre zriaďovanie podúčtov je uzatvorenie a platnosť príslušného dodatku k zmluve o vedení bežného účtu.
2. Prostredníctvom elektronickej správy účtov sa dajú tiež rušiť účty, s výnimkou bežných účtov, Fiokonta, bežných vkladov, špeciálnych bežných účtov a účtov, o ktorých to stanoví Zmluva o vedení účtu alebo Obchodné podmienky pre zriaďovanie a vedenie účtov (vydávané Bankou, príp. vydávané priamo bankou Fio banka, a.s., ak ide o elektronickú správu účtu vedeného priamo bankou Fio banka, a.s.) (ďalej aj len „obchodné podmienky“), aj keď neboli založené pomocou elektronickej správy účtov, pokiaľ sa Banka a klient nedohodnú inak. Aspoň po dobu 360 dní odo dňa zrušenia účtu môže klient naďalej získavať všetky informácie o účte či podúčte, vrátane pohybov na účte či podúčte.

## Čl. V. Rozsah zodpovednosti strán

1. Klient zodpovedá za záväzky vzniknuté elektronickým podaním pokynu rovnako, ako by bol pokyn alebo žiadosť podaná písomne.
2. Klient zodpovedá za logickú správnosť a súlad všetkých svojich elektronicky podaných pokynov so zmluvou a Podmienkami, prípadne ďalšími predpismi.
3. Klient zodpovedá za škodu, ak škodu spôsobil svojím podvodným konaním, úmyselným nesplnením povinnosti používať internetbanking podľa podmienok uvedených v zmluve či Podmienkach, úmyselným nesplnením povinnosti podľa čl. XVI alebo úmyselným porušením povinnosti vykonať všetky primerané úkony na zabezpečenia dôverných údajov, alebo z hrubej nedbanlivosti. Hrubou nedbanlivosťou sa rozume porušenie akejkoľvek povinnosti klienta vyplývajúcej z článku II, III,VIII, IX, XI až XIV, XV a XVI týchto podmienok, najmä porušenie opatrení za účelom zaistenia bezpečnosti a utajenia dôverných údajov, porušenie povinností na zabezpečenie zariadenia používaného pre prístup do internetbankingu či smartbankingu, porušenie povinností na zabezpečenie mobilného zariadenia/SIM karty používanej na zasielanie SMS kódov, porušenie povinnosti overiť adresu serveru Banky, porušenie povinnosti overiť identifikáciu aplikácie pre elektronický podpis, porušenie povinnosti riadne skontrolovať pomocou zeleného symbolu visiaceho zámku nasledovaného názvom „Fio banka, a.s.(CZ)“ alebo zeleného nápisu Fio banka v adresnom riadku internetového prehliadača, že komunikuje so serverom Banky alebo porušenie povinnosti včas oznámiť Banke podozrenie na zneužitie bezpečnostných údajov.
4. Banka zodpovedá za bezchybnosť spracovania požiadaviek klienta, ktoré sú jej odovzdané v súlade so zmluvou a Podmienkami. Banka nenesie žiadnu zodpovednosť za prípadné škody vzniknuté z dôvodu poruchy prenosovej siete alebo z dôvodu náhody, t.j. nepredvídateľnej a na vôli Banky nezávislej udalosti, ktorej následky nemohla Banka odvrátiť.
5. Ak sa neuplatní zodpovednosť podľa čl. V. ods. 3 Podmienok a podmienky uvedené v ustanovení § 12 ods. 3 zákona o platobných službách, klient, ktorý je spotrebiteľom, znáša stratu za všetky neautorizované (neoprávnené) platobné operácie do čiastky zodpovedajúcej 50 EUR, ak bola táto strata spôsobená v dôsledku zneužitia internetbankingu či smartbankingu neoprávnenou osobou v dôsledku nedbanlivosti klienta pri zabezpečovaní dôverných údajov (najmä prihlasovanie meno, heslo, autorizačný sms kód, apod.), t.j. v dôsledku nedbanlivosti pri plnení povinnosti klienta vykonať všetky primerané úkony na zabezpečenia dôverných údajov (ako personalizovaných bezpečnostných prvkov). Klient, ktorý nie je spotrebiteľom, znáša stratu v plnom rozsahu, ktorá súvisí so všetkými neautorizovanými platobnými operáciami vykonanými prostredníctvom internetbankingu či smartbankingu a ktorá je spôsobená zneužitím internetbankingu či smartbankingu neoprávnenou osobou v dôsledku nedbanlivosti klienta pri zabezpečovaní dôverných údajov (najmä prihlasovanie meno, heslo,

autorizačný sms kód, apod.), t.j. v dôsledku nedbanlivosti pri plnení povinnosti klienta vykonať všetky primerané úkony na zabezpečenia dôverných údajov (ako personalizovaných bezpečnostných prvkov); klient, ktorý nie je spotrebiteľom, nesie stratu v plnom rozsahu i v prípade situácií uvedených v ustanovení § 12 ods. 3 zákona o platobných službách. Primeranými úkonmi na zabezpečenie ochrany dôverných údajov sa na účely tohto článku považujú všetky úkony na zabezpečenie ochrany dôverných údajov, ktoré sú uvedené v zmluve a Podmienkach.

6. Banka zodpovedá za bezchybnosť spracovania požiadaviek klienta, ktoré sú jej odovzdané v súlade so Zmluvou a podmienkami. Banka nenesie žiadnu zodpovednosť za prípadné škody vzniknuté v súvislosti s okolnosťou, ktorá je neobvyklá, nepredvídateľná, nezávislá na vôli Banky a ktorej následky nemohla Banka odvrátiť (vrátane takých škôd vzniknutých z dôvodu poruchy prenosovej siete) alebo z dôvodu náhody, t.j. nepredvídateľnej a na vôli Banky nezávislej udalosti, ktorej následky nemohla Banka odvrátiť.
7. Pre zodpovednosť Banky sa ďalej použijú ustanovenia čl. XIII Obchodných podmienok pre zriaďovanie a vedenie účtov, vydaných Bankou.

## Čl. VI. Zmluvná odmena a poplatky

1. Výška odmeny účtovaná Bankou za umožnenie elektronické správy účtov je uvedená v Cenníku finančných operácií a služieb (ďalej tiež len „Cenník“), ktorý vydáva Banka. Cenník môže byť vydaný vo forme niekoľkých čiastkových cenníkov. Náklady na komunikáciu s Bankou hradí klient.
2. Poplatky za vykonané pokyny zadané pomocou elektronickej správy účtov a poplatky za využitie informačných a autorizačných prostriedkov sú rovnako uvedené v Cenníku finančných operácií a služieb.

## Čl. VII. Pokyny a informácie, ktoré sa dajú podávať, resp. získavať prostredníctvom el. správy účtov

1. Prostredníctvom internetbankingu, ktorý slúži ako komunikačný program medzi Bankou a klientom, je klient hlavne oprávnený zadávať pokyny Banke, prijímať od Banky informácie, správy, upozornenia, ponuky na platobné a bankové služby, uzatvárať s Bankou konkrétne zmluvy a tiež inak komunikovať s Bankou. Z toho dôvodu je klient povinný sledovať všetky správy, informácie a upozornenia, ktoré mu Banka prostredníctvom internetbankingu doručí. Neplnenie tejto povinnosti je porušenie povinností vyplývajúcich zo zmluvy.
2. Klient súhlasí s tým, že Banka v prípadoch, kde to právne predpisy nevylučujú, bude používať naskenovaný podpis ako mechanický prostriedok náhrady vlastnoručného podpisu v zmluvných vzťahoch s klientom založených Zmluvou a upravených týmito Podmienkami. Klient berie na vedomie, že takúto prax považuje Banka za obvyklú.
3. Banka i klient súhlasia, že v rámci kontaktu klienta s Bankou prostredníctvom internetbankingu bude autorizácia pokynov klienta v internetbankingu považovaná za mechanický prostriedok náhrady jeho vlastnoručného podpisu, kde to právne predpisy nevylučujú. Klient prehlasuje, že takúto prax berie za obvyklú.
4. Klient súhlasí, že Banka má právo používať internetbanking, e-mailové správy, kuriéra, službu krátkych textových správ (SMS) alebo iný prostriedok diaľkovej komunikácie umožňujúci komunikáciu s klientom s cieľom ponúknuť mu akékoľvek služby spojené so zriadením bežného účtu. Klient súhlasí s poskytnutím akýchkoľvek informácií, materiálov a ponúk spôsobom uvedeným v predchádzajúcej vete tohto odseku.
5. V prípadoch, kedy Banka bude klientovi doručovať akýkoľvek dokument prostredníctvom internetbankingu, bude sa dokument považovať za doručený v momente, keď Banka dostane potvrdenie o jeho prečítaní zo strany klienta, najneskôr však dňom nasledujúcom po odoslaní dokumentu, pokiaľ klient nepreukáže, že sa z dôvodov nezávislých na jeho vôli nemohol s obsahom zaslaného dokumentu zoznámiť.
6. V prípadoch doručovania kuriérom sa považuje za deň doručenia deň prijatia zásielky klientom.

7. Ak je príslušná služba Bankou poskytovaná a ak nie je ďalej uvedené inak, v internetbankingu sa dajú podávať najmä tieto pokyny:
a) podanie/zmena/rušenie riadnej výpovede na vklad s výpovednou lehotou alebo na sporiaci účet s výpovednou lehotou,
b) prevodný príkaz (príkaz na prevod finančných prostriedkov),
c) odvolanie prevodného príkazu, ktorého splatnosť ešte len nastane,
d) trvalý prevodný príkaz z bežného účtu alebo bežného vkladu,
e) zmena/rušenie trvalého prevodného príkazu z bežného účtu alebo bežného vkladu,
f) zriadenie/zmena/zrušenie súhlasu s inkasom v prospech iného účtu,
g) zriadenie/zmena/zrušenie súhlasu s platbami SIPO,
h) avizovanie výberu hotovosti pobočke Banky,
i) zriaďovanie podúčtov a rušenie podúčtov, rušenie účtov[1] s výnimkou účtov podľa čl. IV. ods. 2 Podmienok,
j) zmena spôsobu pripisovania úrokov, dispozícia s úrokmi a dispozícia so zostatkom účtu alebo podúčtu po jeho zrušení,
k) zmena hesla (pre internetbanking či smartbanking),
l) splnomocnenie tretej osoby na správu účtu majiteľa,
m) zriadenie/zrušenie SMS a e-mailového upozornenia o udalostiach na účte,
n) zriadenie/zrušenie smartbankingu a zadanie prístupového hesla pre smartbanking a UID mobilného zariadenia pre smartbanking,
o) zriadenie/zmena/zrušenie PINu pre smartbanking,
p) zmena UID mobilného zariadenia pre smartbanking,
q) zmena spôsobu a frekvencie zasielania výpisov z účtov,
r) prijímať predschválené ponuky Banky na poskytnutie ďalších služieb v rámci zriadenia bežného účtu či podúčtu,
s) zaslať Banke návrh na uzatvorenie zmluvy o poskytovaní bankových či platobných služieb,
t) povolenie/zakázanie vykonávania pokynov uvedených v ods. 1b. čl. III Podmienok bez autorizácie pomocou bezpečnostného prvku a prípadne s tým súvisiace ďalšie pokyny,
u) uzatvorenie zmluvy o vydaní platobnej karty a ďalších zmlúv podľa aktuálnej ponuky,
v) voľba/zmena vlastného PINu,
w) zmena výšky limitu pre platobné karty,
x) stavu platobnej karty,
y) voľba použitia biometrického snímača v mobilnom zariadení pre smartbanking (toto možno nastaviť iba cez smartbanking)
z) zriadenie/zrušenie tokenu pre službu API,
aa) zadanie/zmenu/zrušenie korešpondenčnej adresy,
bb) zadanie/zrušenie kontaktného telefónu,
cc) zadanie/zrušenie kontaktného e-mailu,
dd) zmenu pobočky, na ktorej je evidovaná dokumentácia klienta,
ee) ak to umožňuje Banka, uzatvorenie dodatkov k skôr uzatvoreným zmluvám.
8. Elektronickou správou účtov sa dajú získavať najmä tieto informácie:
a) parametre účtov a podúčtov,
b) zostatok na účte alebo podúčte k určitému dátumu,
c) pohyby na účte alebo podúčte za určité obdobie (správy o zúčtovaní položiek),
d) výpis z účtu alebo podúčtu,
e) parametre vydanej platobnej karty,
f) prehľad podaných pokynov spolu s ich stavmi, a pod.
9. Niektoré z pokynov podľa ods. 7, podľa požiadaviek Banky týkajúcich sa autorizácie a aktuálnych v čase zadávania pokynu, musia byť autorizované podľa čl. III. Podmienok.

[1] Rušiť účty, prípadne inak nakladať s účtami, môže iba majiteľ účtu a osoba na to majiteľom účtu splnomocnená.

Niektoré z pokynov a informácií, ktoré možno podávať resp. získavať prostredníctvom el. správy účtov, uvádzané v ods. 7 a 8, môžu byť pri použití smartbankingu obmedzené v závislosti od verzie aplikácie, mobilného zariadenia či jeho operačného systému. Banka je oprávnená (nie však povinná) niektoré pokyny uvedené v tomto článku VII umožniť podať tiež neplnoletým klientom (ide napr. o pokyny alebo požiadavky súvisiace s SMS a emailovým upozornením, vydanou platobnou kartou k danému účtu či smartbankingom); Na základe žiadosti zákonného zástupcu je Banka oprávnená niektoré pokyny podľa ods. 7 tohto článku umožniť neplnoletému klientovi tiež autorizovať, a to spôsobom podľa čl. III ods. 3 podmienok B a v rozsahu limitov podľa čl. 14 tohto článku. Neplnoletým klientom sa pre účely autorizácie pokynov podľa tohto odseku považuje osoba, ktorá dovŕšila 15 rokov a neprekročila 18 rokov veku. Banka je oprávnená rozsah pokynov, ktoré je možné podať alebo autorizovať neplnoletým klientom, podľa vlastného uváženia rozšíriť aj zúžiť.

10. Elektronickou správou účtov je možné zadať požiadavku na založenie alebo zrušenie SMS a e-mailového upozornenia o niektorých udalostiach na účte. Klient si môže zvoliť upozornenie podľa aktuálnej ponuky prístupnej klientovi v rámci elektronickej správy účtov. Klient je oprávnený zvoliť možnosť zasielania informácií o udalostiach na účte formou sms alebo e-mailu na ním zadaný kontakt. Banka je oprávnená (nie však povinná) i bez predchádzajúceho upozornenia jednostranne zrušiť SMS a e-mailové upozornenie, ak dôjde k vzniku neoprávneného debetného zostatku na účte klienta; po vyrovnaní debetného zostatku sa SMS a e-mailové upozornenie neobnovuje – pre obnovenie služby je potrebné nové založenie SMS a e-mailového upozornenia, ktoré môže klient vykonať po vyrovnaní debetného zostatku. Upozornenie podľa tohto odseku založené oprávnenou osobou sa neruší so zánikom oprávnenia tejto osoby; pre zrušenie upozornenia je potrebné podať pokyn zo strany aktuálne oprávnenej osoby.
11. Príkazom k úhrade sa pre účely Podmienok rozumie aj príkaz k tzv. dobitiu kreditu (ak podanie takého príkazu Banka umožňuje; Banka môže takýto príkaz označiť aj iným obdobným názvom zrozumiteľným pre bežného klienta), tj. príkaz k úhrade finančných prostriedkov v prospech účtu príslušného mobilného operátora za účelom dobitia kreditu SIM karty (tj. za účelom predplatenia služieb poskytovaných mobilným operátorom jeho zákazníkovi) identifikovanej klientom pri zadávaní pokynu uvedením telefónneho čísla príslušnej SIM karty; klient pri zadaní pokynu nezadáva číslo účtu mobilného operátora (príjemcu prevodu), ale zadá telefónne číslo príslušnej SIM karty, ktorej kredit má byť prevodom dobitý, prípadne určí aj príslušného mobilného operátora (ak je to vyžadované) a zadá iné Bankou požadované údaje.
12. Banka si vyhradzuje právo obmedziť dispozíciu s peňažnými prostriedkami na účte (popr. s určitou výškou peňažných prostriedkov) prostredníctvom internetbankingu či smartbankingu, a to najmä z dôvodu výkonu rozhodnutia či z dôvodu exekúcie. Pokaľ je dispozícia s peňažnými prostriedkami na účte podľa predchádzajúcej vety obmedzená a majiteľ účtu má zákonný nárok na výplatu peňažných prostriedkov (napr. prostriedky nepodliehajúce exekúcii prikázaním pohľadávky z účtu v banke), Banka je oprávnená, nie však povinná, zamedziť ich vyplácaniu prostredníctvom internetbankingu či smartbankingu a vyžadovať, aby majiteľ účtu tento nárok uplatnil na pobočke Banky; Banka má však právo (nie povinnosť) umožniť vyplatenie takejto čiastky i prostredníctvom internetbankingu či smartbankingu, a to i v prípade, keď účet majiteľa spravuje osoba odlišná od majiteľa účtu – pre prípad takého postupu k tomu majiteľ účtu splnomocnenú osobu v zmysle čl. I. ods. 1 týchto Podmienok splnomocňuje.
13. Ak nie je v týchto Podmienkach stanovené výslovne inak, a ak nie je v splnomocnení udelenom v zmysle čl. I. ods. 1 týchto Podmienok výslovne stanovené, že splnomocnenie nezaniká úmrtím majiteľa účtu, splnomocnenie udelené podľa čl. I. ods. 1 týchto Podmienok zaniká úmrtím majiteľa účtu. Banka a klient sa dohodli, že v deň nasledujúci po dni, keď sa Banka hodnoverne dozvie o úmrtí majiteľa účtu (resp. o jeho vyhlásení za mŕtveho), zruší oprávnenie k elektronickej správe účtov v zmysle čl. I. ods. 1 týchto Podmienok.
14. Klient je oprávnený prostredníctvom písomnej žiadosti (na ľubovoľnej pobočke Banky či korešpondenčne s úradne overenými podpismi) nastaviť maximálny denný a mesačný limit

majiteľa a limit príkazcu (na účely tohto odseku tiež len "limit") pre elektronicky podané pokyny (počiatočný limit nie je zo strany Banky nastavený) a toto nastavenie následne aj meniť; v takom prípade je možné elektronické pokyny podať prostredníctvom internetbankingu a smartbankingu v súčte za všetky pokyny iba do výšky aktuálne nastaveného limitu, ak nie je uvedené inak. "Limit majiteľa" je limit nastavený klientovi ako majiteľovi účtu; tento limit platí súhrnne pre všetky účty vedené pre tohto klienta bez ohľadu na to, či bol pokyn podaný klientom alebo akýmkoľvek splnomocnencom (vrátane zákonného zástupcu). "Limit príkazcu" je limit nastavený klientovi ako užívateľovi internetbankingu, resp. smartbankingu; tento limit platí súhrnne pre všetky pokyny podané užívateľom bez ohľadu na to, k akému účtu bol pokyn podaný. Banka je oprávnená niektoré typy pokynov nezapočítavať do nastaveného limitu (ide najmä o príkazy na inkaso, avizovanie výberu hotovosti či prevody medzi účtami klienta). Elektronicky podaný pokyn v inej mene ako EUR bude na účely tohto odseku prepočítaný kurzom ECB aktuálnom k okamihu podania pokynu. Banka je oprávnená nastaviť konkrétnemu klientovi maximálny denný a mesačný limit aj bez jeho výslovnej žiadosti (najmä v prípade neplnoletých osôb alebo opatrovníctva); výška takých limitov je stanovená bankou. Maximálna výška denného limitu aj mesačného limitu v prípade neplnoletého klienta je 550 EUR; Banka je oprávnená stanovené limity individuálne zmeniť. Banka si vyhradzuje právo jednostranne meniť limity uvedené v tomto odseku, vrátane zníženia nastavených limitov, a to aj individuálne vo vzťahu ku konkrétnemu klientovi. Dôvodom prípadného individuálneho zníženia limitov zo strany Banky môže byť najmä porušenie Zmluvy, týchto podmienok, výkon rozhodnutia alebo exekúcie, zvýšenie rizika neschopnosti splácania záväzkov klientom, a pod. Po pominutí pôvodných dôvodov pre zníženie limitu je Banka oprávnená, nie však povinná, aj bez žiadosti klienta upraviť limity na hodnoty platné pred ich znížením zo strany Banky.

## Čl. VIII. Bezpečnostné upozornenia súvisiace s využívaním internetbankingu

1. V súvislosti s využívaním elektronických komunikačných služieb si Banka dovoľuje informovať klienta o niektorých bezpečnostných rizikách s tým spojených a zároveň si dovoľuje upozorniť klienta na základné možnosti, ktorými môže ako užívateľ ochrániť svoje osobné údaje, prihlasovacie meno a prístupové heslo do internetbankingu, elektronický kľúč, heslo chrániace elektronický kľúč, PIN pre smartbanking, prípadne zaslaný sms kód, e-PIN (pre platby kartou), telefónne číslo, UID mobilného zariadenia, kód (passcode, PIN) pre prístup k mobilnému zariadeniu, token pre službu API a iné dôverné alebo citlivé údaje (ďalej tiež „dôverné údaje“) a zariadenie pred ich zneužitím. Ide o základné pravidlá, ktoré je potrebné dodržiavať na ochranu dôverných údajov a zariadenia klienta.
2. Banka a klient berú na vedomie, že zaistenie bezpečnosti dôverných informácií pri využívaní elektronických komunikačných služieb je zodpovednosťou obidvoch zmluvných strán v rozsahu ich sféry vplyvu, a že zavedenie a dodržiavanie niektorých preventívnych opatrení môže vyžadovať finančné náklady.
3. Banka je povinná na svoje náklady vykonať vo svojej sfére vplyvu také technické a organizačné opatrenia za účelom zaistenia bezpečnosti dôverných údajov, ktoré sú s ohľadom na obvyklé riziká porušenia ochrany dôverných údajov technicky možné a primerané.
4. Klient je povinný na svoje náklady vykonať vo svojej sfére vplyvu také technické opatrenia za účelom zaistenia bezpečnosti dôverných údajov, ktoré sú s ohľadom na obvyklé riziká porušenia ochrany dôverných údajov technicky možné a primerané. Klient berie na vedomie riziká spojené s využívaním elektronických komunikačných služieb a zaväzuje sa dodržiavať hlavne nižšie uvedené preventívne a bezpečnostné opatrenia a postupy na zabezpečenie bezpečnosti dôverných údajov. Nedodržanie týchto pravidiel a opatrení môže viesť k zneužitiu dôverných údajov a k vzniku škody klientovi alebo tretej osobe.
5. S ohľadom na čo najvyššiu ochranu dôverných údajov a majetku klienta odporúča Banka, aby si klient dohodol s Bankou autorizáciu elektronických pokynov pomocou sms správ alebo

autorizáciu prostredníctvom elektronického podpisu a aby využíval pre zadávanie svojho hesla pri prihlasovaní do internetbankingu grafickú klávesnicu.

## Čl. IX. Riziká plynúce z využívania elektronických komunikačných služieb

1. Elektronické komunikačné služby sú poskytované prostredníctvom dátových prípadne telefónnych liniek (ďalej tiež „dátové linky“), ktoré neprevádzkuje Banka, ale tretia osoba odlišná od Banky. Zabezpečenie týchto dátových liniek je mimo sféry vplyvu Banky a Banka preto nie je schopná úplne zabrániť všetkým možným rizikám zneužitia dôverných údajov v priebehu prenosu prostredníctvom dátovej linky. Pri prenose dôverných údajov nemožno preto úplne vylúčiť riziko neoprávneného získania dôverných informácií treťou osobou (napr. hrozba tzv. hackerov, interné riziká prevádzkovateľa dátovej siete, tzv. Man in the middle, t.j. odpočúvanie komunikácie treťou osobou predstierajúcou protistranu komunikácie, odpočúvanie telefonických hovorov, podvrhnutie dát a pod.).
2. Niektoré riziká plynúce z využívania elektronických komunikačných služieb môžu byť tiež vo sfére vplyvu klienta. Medzi tieto riziká patrí predovšetkým nedostatočné zabezpečenie zariadenia klienta, ktorý je používaný pre prihlásenie do internetbankingu, smartbankingu a na podávanie pokynov Banke a ďalej nesprávne nakladanie s dôvernými údajmi klientom a z toho plynúca možnosť ich zneužitia zo strany tretích osôb.
3. Banka nezodpovedá za prípadnú škodu klienta alebo tretích osôb vzniknutú zneužitím dôverných informácií neoprávnene získaných z dátových liniek mimo sféru vplyvu Banky, zariadenia klienta alebo v dôsledku nesprávneho nakladania s týmito údajmi klientom, pokiaľ nejde o prípad porušenia povinností na strane Banky.

## Čl. X. Preventívne opatrenia vykonávané Bankou

1. Banka vykonáva vo svojej sfére vplyvu preventívne opatrenia znižujúce riziko zneužitia dôverných informácií.
   Medzi tieto opatrenia patrí hlavne šifrovanie všetkých dát (t.j. napr. užívateľské meno a heslo, informácie o pohyboch, účtoch atď.), ktoré sú prenášané medzi zariadením klienta a serverom Banky. Všetky prenášané dáta sú šifrované štandardizovanými algoritmami s minimálne 128 bitovými kľúčmi. Šifrovanie prenášaných dát výrazne znižuje možnosť zistenia dôverných údajov o klientovi treťou osobou pri prenose dátovou linkou a ich následného zneužitia.
2. Banka ďalej umožňuje klientovi využívať ďalšie bezpečnostné prvky chrániace prístup do internetbankingu, medzi ktoré patrí možnosť využitia grafickej klávesnice pre zadávanie hesla pri prihlasovaní do internetbankingu, čo znižuje riziko neoprávneného zistenia týchto údajov treťou osobou a možnosť potvrdzovania elektronických pokynov klienta, podľa Protokolu o nastavení autorizácie elektronických pokynov, formou sms správ na individuálne stanovené telefónne číslo klienta alebo formou elektronického podpisu.
3. Informácie o niektorých bezpečnostných opatreniach sú uvedené tiež na prihlasovacej stránke do internetbankingu.

## Čl. XI. Utajenie dôverných údajov

1. Klient je povinný chrániť svoje dôverné údaje pred zverejnením a zneužitím.
2. Klient je povinný nezaznamenávať si dôverné údaje. Ak si však klient dôverné údaje napriek tomu zaznamená, je povinný ich uschovať samostatne od ostatných dôverných údajov a na takom mieste, ktoré nie je voľne prístupné tretím osobám.
3. Klient je povinný neuvádzať dôverné údaje tak, aby sa dali spojiť s príslušným účtom (napr. napísanie dôverných údajov v dokladoch spojených s účtom, automatické zapamätanie prihlasovacieho mena a hesla do internetbankingu zariadením).
4. Klient je povinný dodržiavať dostatočnú mieru obozretnosti pri správe dôverných údajov, predovšetkým nezadávať dôverné údaje pred inou osobou, neoznamovať dôverné údaje iným osobám, a to ani rodinným príslušníkom a blízkym osobám. Za porušenie týchto Podmienok sa

však nepovažuje oznámenie užívateľského mena inej fyzickej osobe za účelom zriadenia oprávnenia k účtu tejto osoby, resp. k účtu ovládanému touto osobou.

5. Klient je povinný si zvoliť heslo ako kombináciu čísiel a veľkých a malých písmen, bez osobného vzťahu k svojej osobe či k blízkym osobám. Jednoduché heslo s osobnými rysmi je ľahšie odhaliteľné. Klient nesmie použiť ako heslo a PIN pre smartbanking svoj dátum narodenia, rodné číslo, telefónne číslo, po sebe idúce číslice apod. Klient je povinný heslo a PIN pre smartbanking pravidelne meniť, ak nie je ďalej ustanovené inak. Klient si môže zmeniť heslo iba v internetbankingu či smartbankingu, ak to banka umožňuje. Banka nebude v žiadnom prípade vyžadovať od klienta iný postup. Prvé heslo (vrátane obnoveného hesla) je klient povinný si zmeniť pri prvom prihlásení do internetbankingu po vydaní tohto hesla. Prvé heslo (vrátane obnoveného hesla) je klientovi poskytnuté postupom stanoveným Bankou (postup môže byť stanovený všeobecne alebo aj vo vzťahu k určitému typu zmlúv, napr. uzatvorených online), a to napr. v papierovej podobe (prípadne aj priamo v zmluvnej dokumentácii) či v elektronickej podobe (napr. v rámci zaheslovaného súboru zaslaného na e-mailovú adresu uvedenú klientom). Za účelom aktivácie prvého / obnoveného hesla je Banka oprávnená zaslať klientovi sms na telefónne číslo pre autorizáciu (prípadne na telefónne číslo, ktoré klient za týmto účelom Banke uvedie), ktorej súčasťou je ďalší bezpečnostný prvok (či bezpečnostné prvky), ktorými môžu byť napr. párovací kód (Banka je tento kód oprávnená od klienta vyžadovať napr. za účelom zaslania zaheslovaného súboru s heslom, prípadne aj s loginom, za účelom odovzdania hesla v papierovej podobe priamo na pobočke Banky či za účelom aktivácie poskytnutého hesla) alebo špeciálne heslo na otvorenie zaheslovaného súboru zaslaného na e-mailovú adresu klienta; Banka je oprávnená z bezpečnostných dôvodov vydať klientovi nové prvé (resp. obnovené) heslo v prípade zmeny autorizačného telefónneho čísla. Banka je oprávnená z bezpečnostných dôvodov platnosť prvého hesla (vrátane obnoveného hesla) obmedziť na Bankou stanovenú dobu, a to vrátane už vydaných hesiel (napr. 7 kalendárnych dní od vydania tohto hesla alebo od uvedenia bezpečnostného prvku poskytnutého Bankou zo strany klienta, napr. párovacieho kódu); Banka je oprávnená stanovenú dobu platnosti týchto hesiel kedykoľvek zmeniť. Platnosť nasledujúceho hesla je z bezpečnostných dôvodov obmedzená na 365 dní, ak nie je ďalej ustanovené inak. Ak vyprší uvedené lehota, bude klient pri najbližšom prihlásení do internetbankingu či smartbankingu vyzvaný k zmene hesla. Ak má klientovo aktuálne heslo do internetbankingu či smartbankingu aspoň 12 znakov, banka je oprávnená (nie však povinná) považovať také heslo za platné aj potom, čo uplynie doba platnosti udeleného hesla podľa tohto odseku, a to až na dobu neobmedzene dlhú. V takom prípade klient nebude po prihlásení do aplikácie internetbanking či smartbanking vyzvaný na zmenu hesla. Banka odporúča, aby klient nepoužíval pre rôzne aplikácie (najmä internetbanking a smartbanking, ale aj iné typy aplikácií, ako napr. e-mailová schránka, sociálne siete, hry a pod.) rovnaké prístupové heslá, najmä, aby takáto zhoda hesiel nebola medzi aplikáciou s prístupom k účtu a akoukoľvek inou používanou aplikáciou.
6. Klient je povinný dodržiavať dostatočnú mieru obozretnosti pri zadávaní dôverných údajov, predovšetkým nezasielať dôverné údaje pomocou e-mailu, sms, sociálnych sietí (napr. Facebook, Twitter, LinkedIn) či aplikácií pre vzdialenú komunikáciu (napr. Skype, ICQ), nezadávať ich na inej internetovej stránke, než na stránke určenej na prihlasovanie do internetbankingu, a to ani v prípade, ak klient obdrží e-mail či sms, či správu, ktorá napodobňuje výzvu, najmä od Banky, na zaslanie dôverných údajov alebo na ich vyplnenie na inej internetovej stránke. Banka takýto druh správ v žiadnom prípade nebude posielať svojim klientom.

## Čl. XII. Uloženie elektronického kľúča a tokenu pre službu API

1. Prostredníctvom tokenu pre službu API je klient, resp. osoba disponujúca tokenom pre službu API, oprávnená získavať informácie o účte, zadávať pokyny k úhrade (nie však také pokyny autorizovať) alebo vykonávať iné úkony bez prihlásenia do internetového bankovníctva (bez uvedenia prihlasovacieho mena a prístupového hesla). Bližšie informácie o službe API a tokenu

pre službu API sú uvedené na internetových stránkach Banky. Klient je povinný chrániť svoj elektronický kľúč, ktorý používa pri autorizácii pokynov, a token pre službu API proti jeho zneužitiu, najmä proti jeho odcudzeniu, skopírovaniu a pod. Zneužitím elektronického kľúča klienta alebo tokenu pre službu API môže iná osoba predstierať identitu klienta a zadávať či autorizovať pokyny v mene klienta popr. vykonávať ďalšie úkony v mene klienta. Zneužitie elektronického kľúča alebo tokenu pre službu API môže spôsobiť klientovi škodu. Token pre službu API k účtu klienta – fyzickej osoby zaniká úmrtím majiteľa účtu. Banka a klient sa dohodli, že najneskôr v najbližší pracovný deň nasledujúci po dni, keď sa Banka hodnoverne dozvie o úmrtí majiteľa účtu (resp. o jeho vyhlásení za mŕtveho), zruší token pre službu API k účtu klienta – fyzickej osoby. Zrušením príslušného účtu, ku ktorému je zriadený token pre službu API, nedochádza automaticky k zrušeniu tokenu pre službu API (klient je teda oprávnený získavať informácie o účte prostredníctvom tokenu pre službu API aj po zrušení príslušného účtu); pre zrušenie tokenu pre službu API je potrebné podať pokyn zo strany oprávnenej osoby.

2. Klient je povinný elektronický kľúč a token pre službu API uchovávať iba na zabezpečenom mieste (napr. počítač server, prenosné médium atď.), o ktorom si môže byť s dostatočnou mierou istý, že je chránený pred možnými hrozbami plynúcimi z pripojenia k dátovej sieti. Klient má povinnosť uchovávať elektronický kľúč iba na zašifrovanom disku alebo elektronický kľúč zašifrovať. Klient nesmie uchovávať a používať elektronický kľúč a token pre službu API na mieste, ktoré je voľne (bez vedomia či povolenia klienta) prístupné tretím osobám.
3. Ak klient uchováva elektronický kľúč alebo token pre službu API na prenosnom médiu, klient je povinný toto médium uložiť na miesto, kde je do veľkej miery obmedzené riziko jeho zneužitia, najmä odcudzenia, skopírovania či poškodenia.
4. Rozsah zodpovednosti strán je vymedzený v čl. V. týchto Podmienok. Klient je vždy zodpovedný za spôsobenú škodu v súvislosti s použitím tokenu pre službu API treťou osobou, najmä pokiaľ klient tretej osobe token pre službu API sprístupnil.

## Čl. XIII. Bezpečnostné opatrenia vo sfére vplyvu klienta, zabezpečenie zariadenia klienta

1. Klient je povinný dodržiavať všetky povinnosti, ktoré sú stanovené v ods. 2 až 10 tohto článku. Všetky informácie obsiahnuté v ods. 2 až 10 tohto článku sú pre klienta povinnosťami, ak nie je pri niektorej z nich výslovné uvedené inak.
2. Klient je povinný používať internetbanking iba na zariadeniach, ktoré sú riadne zabezpečené proti zneužitiu dôverných údajov. Klient nesmie používať internetbanking hlavne v internetových kaviarňach a na iných verejne prístupných zariadeniach, ani na zariadeniach, u ktorých klient nemá dostatočnú mieru istoty, že sú zabezpečené proti zneužitiu dôverných údajov. Klient má povinnosť odhlásiť sa z internetbankingu vždy bezprostredne po ukončení práce s ním a nikdy neponechávať mimo dohľad svoje zariadenie, pokiaľ je klient prihlásený do internetbankingu.
3. Klient je povinný sa pred prihlásením do internetbankingu riadne presvedčiť, že komunikuje so správnym poskytovateľom služby. Klient je povinný vždy si overiť, že v adresnom riadku prehliadača je adresa začínajúca: https://ib.fio.cz/ib/, https://ib.fio.sk/ib/, a stránka používa šifrované spojenie so serverom Banky za použitie platného certifikátu SSL servera. Táto skutočnosť je indikovaná pomocou zeleného symbolu visiaceho zámku nasledovaného názvom „Fio banka, a.s. (CZ)“ alebo zeleným nápisom Fio banka v adresnom riadku internetového prehliadača. Názorný príklad overenia platnosti certifikátu podľa tohto odseku je dostupný na: http://www.fio.sk/docs/sk/fingerprint-sk.pdf. Tu je dostupný i príklad overenia identifikácie serveru Banky prostredníctvom tzv. SHA 1 Fingerprintu (toto overenie však nie je povinné, i keď je doporučené). V prípade aplikácie smartbanking je klient povinný overiť identitu poskytovateľa a autora aplikácie pri jej inštalácii do mobilného zariadenia, pri pripojení na server Banky prostredníctvom aplikácie smartbanking už klient overenie identifikácie serveru Banky nevykonáva. Banka nezodpovedá za škodu spôsobenú porušením povinností stanovených

v tomto odseku klientom. Banka má právo kedykoľvek obmedziť prístup na ktorúkoľvek z adries uvedených v tomto odseku, a to dočasne aj natrvalo.

4. Klient je pri každom svojom pripojení aplikáciou Fio-podpis (ďalej tiež „elektronický kľúč“) povinný overiť jej identifikáciu (SHA1 Fingerprint) porovnaním so správnou identifikáciou, ktorá je dostupná na: http://www.fio.sk/docs/sk/fingerprint-sk.pdf. Banka nezodpovedá za škodu spôsobenú porušením tejto povinnosti klientom. Identifikácia Fio-podpisu je zobrazená v okne prostredia JAVA pri spustení aplikácie Fio-podpis, alebo - v prípade prijatia tohto certifikátu za dôveryhodný – v dôveryhodných certifikátoch v prostredí JAVA.
5. Klient má povinnosť v prípade akýchkoľvek pochybností o tom, že komunikuje s Bankou, alebo že spojenie nie je riadne zabezpečené, nevykonávať žiadne úkony, ktoré by mohli viesť k prezradeniu alebo zneužitiu dôverných údajov, predovšetkým zadanie prihlasovacích údajov.
6. Klient je povinný zabezpečiť na zariadení, na ktorom sa rozhodne používať internetbanking, a kde je to technicky možné, aspoň antivírus a funkčný firewall a tieto ochranné prvky pravidelne aktualizovať. Klient je povinný pravidelne sledovať na stránkach Banky (viď. čl. X ods. 3 Podmienok) alebo v správach v internetbankingu, popr. smartbankingu informácie o nových hrozbách a je povinný sa podľa poskytnutých informácii chovať, vrátane povinnosti aktualizovať operačný systém na zariadení, na ktorom sa používa internetbanking. Klient je povinný čítať varovné oznámenia a upozornenia, ktoré mu Banka pošle prostredníctvom e-mailu alebo sms. Pokiaľ varovné oznámenie alebo upozornenie odoslané Bankou podľa predchádzajúcej vety obsahuje informácie, ktorým klient nerozumie, alebo obsahuje popis činnosti, ktorú klient nevykonával alebo si klient nie je istý, či takú činnosť vykonával, alebo obsahuje inú informáciu vzbudzujúcu podozrenie, že došlo k neoprávnenej manipulácii s účtom, alebo obsahuje priamo výzvu na kontaktovanie Banky, je klient povinný kontaktovať Banku za použitia overiteľných kontaktných údajov Banky (prednostne na telefónne číslo +421 2 2085 0310). Banka vo varovnom oznámení a upozornení poslanom prostredníctvom e-mailu alebo sms nebude z bezpečnostných dôvodov uvádzať konkrétne kontaktné údaje.
7. Klient je povinný pre prístup do internetbankingu používať dôveryhodný internetový prehliadač, ktorý pravidelne aktualizuje. Klient je povinný nemeniť pôvodné zabezpečenie internetového prehliadača na zabezpečenie menej bezpečné. Klient je povinný skontrolovať vždy pred zadaním prihlasovacích údajov na prihlasovacej stránke internetbankingu, či internetový prehliadač nehlási akékoľvek varovanie spojené s certifikátom (neaktuálny alebo nedôveryhodný certifikát alebo certifikát vydaný pre inú inštitúciu než Banku). Postup pre zistenie podrobností týkajúcich sa certifikátu je dostupný na: http://www.fio.sk/docs/sk/fingerprint-sk.pdf.
8. Klient má povinnosť vyvarovať sa používaniu internetbankingu na operačných systémoch a prehliadačoch, ktoré daný výrobca už nepodporuje. Klient má povinnosť udržiavať operačný systém zariadení, na ktorých používa internetbanking, a používaný internetový prehliadač s najnovšími nainštalovanými aktualizáciami od výrobcu. Klient je povinný nepoužívať internetbanking na zariadeniach vyžívajúcich verzie operačného systému Windows 7 a staršie.
9. Klient je povinný na zariadeniach, na ktorých používa internetbanking, vyvarovať sa sťahovaniu nedôveryhodných súborov a inštalovaniu nedôveryhodných programov. Klient je povinný na zariadeniach, na ktorých používa internetbanking, navštevovať iba známe, dôveryhodné a bezpečné stránky na internete, neotvárať prílohy doručených e-mailov s podozrivým predmetom, odosielateľom alebo obsahom (textom e-mailu) na takýchto zariadeniach; príkladný zoznam niektorých relevantných indícii je uvedený v odseku 12 tohto článku – ide však iba o demonštratívny zoznam a pri posudzovaní podozrivosti e-mailu sa klient nesmie obmedziť iba na tam uvedené indície. Klient má povinnosť nepoužívať k prístupu do internetbankingu odkaz otváraný zo sociálnych sieti, e-mailov, sms, aplikácii pre vzájomnú komunikáciu či internetových vyhľadávačov (Google, a pod.). Banka nebude v žiadnom prípade zasielať odkazy na stránku určenú k prihlasovaniu do internetbankingu prostredníctvom sociálnych sietí, e-mailov, sms či aplikácií pre vzájomnú komunikáciu. Banka odporúča, aby

klient používal vo svojej e-mailovej schránke spam filter (používanie spam filtru znižuje pravdepodobnosť obdržania e-mailu, ktorý obsahuje vírus či iný škodlivý obsah).

10. Na vyspelejšom mobilnom zariadení (najmä tzv. smartphony a tablety) s operačným systémom iOS, Android, Windows Phone a podobným operačným systémom, na ktorých sa používa internetbanking, smartbanking alebo SIM karta obsahujúca telefónne číslo určené k prijímaniu autorizačných sms kódov od Banky, je klient povinný neinštalovať aplikácie z iných než oficiálnych zdrojov pre príslušný operačný systém mobilného zariadenia (napr. Apple App Store, Google Play, Window Phone Store, atď.) Banka však upozorňuje, že klient sa nemôže spoliehať na kontrolu vykonávanú prevádzkovateľom operačného systému vo vzťahu ku všetkým aplikáciám.
11. Banka odporúča klientovi priebežne sa oboznamovať s aktuálnymi informáciami o možnostiach zabezpečenia zariadenia a o aktuálnych rizikách, ktoré pri používaní zariadenia hrozí. V prípade, ak klientove znalosti tejto problematiky nie sú na riadne zabezpečenie zariadení dostačujúce, resp. ak sám klient má o ich dostatočnosti pochybnosti, Banka odporúča klientovi obrátiť sa s požiadavkou na zabezpečenie zariadenia a jeho prípadného komunikačného príslušenstva na odborníka.
12. Podozrivé či falošné e-maily, v ktorých podvodníci predstierajú konanie Banky alebo iného subjektu, môžu byť indikované napríklad tým, že:
    a) obsahujú odkaz na internetovú stránku, kde názov odkazu nekorešponduje so skutočnou adresou internetových stránok (po umiestnení kurzoru myši nad odkaz sa ukáže skutočná internetová adresa),
    b) obsahujú výzvu vyžadujúcu okamžité konanie adresáta (napr. zaplatenie poplatku, inštaláciu aplikácie, hrozbu exekúcie na majetok, pokiaľ sa okamžite neuhradí atď.),
    c) obsahujú v texte e-mailu zjavné gramatické a pravopisné chyby,
    d) obsahujú neurčité či nedôveryhodné kontaktné údaje odosielateľa,
    e) obsahujú text v neočakávanom jazyku (napr. e-mail od exekútora v anglickom jazyku),
    f) ponúkajú veľmi výhodné podmienky, zárobky, odmeny, pôžičky či investície, veľmi lacný tovar atď.,
    g) v prípade e-mailu poslaného údajne Bankou obsahuje taký e-mail prílohy typu .exe, .zip, .rar, .ppt atď. (také prílohy Banka neposiela),
    h) vyzývajú k zadaniu osobných údajov klienta, hesla alebo PINu, alebo
    i) v e-maile je priamo preklik na vstupný formulár do internetového bankovníctva.

## Čl. XIV. Zabezpečenie sms a mobilného zariadenia

1. Pre prijímanie autorizačných sms kódov je najdôležitejšia SIM karta, ktorá obsahuje telefónne číslo, ktoré ste určili na prijímanie autorizačných sms kódov od Banky (ďalej len „SIM karta“).Banka odosiela autorizačné sms na takto určené telefónne číslo, za samotné doručenie autorizačného sms kódu však nenesie zodpovednosť, a teda nezodpovedá ani za prípadnú škodu klienta vzniknutú nedoručením autorizačného sms kódu. Klient je povinný používať na prijímanie autorizačných sms kódov takú SIM kartu, na ktorú je možné bezproblémovo doručovať SMS správy odosielané prostredníctvom mobilných operátorov poskytujúcich legálne služby na území Slovenskej republiky; plnenie tejto povinnosti však banka nekontroluje a dôsledok jej prípadného porušenia ide plne na ťarchu klienta. Banka najmä upozorňuje, že v prípade prijímania autorizačných sms kódov prostredníctvom SIM karty zahraničného operátora existuje zvýšené riziko nedoručenia autorizačných sms kódov na takúto SIM kartu.
2. Klient je povinný brániť zneužitiu mobilného zariadenie či SIM karty a prijať všetky opatrenia k ich ochrane.
3. Klient je povinný vyvarovať sa požičiavaniu mobilného zariadenia či SIM karty tretím osobám bez toho, aby ste mal neustálu kontrolu nad ich nakladaním s mobilným zariadením a SIM kartou.

4. V prípade, že hrozí riziko, že by klient mohol ponechať mobilné zariadenie mimo svoj dohľad, je povinný znemožniť jeho používanie tretím osobám kódom PIN a tento kód uchovávať v tajnosti a neoznamovať ho tretím osobám, ani si ho nikam nepoznamenávať.
5. Autorizačný kód, ktorý klientovi je doručený Bankou, si klient nesmie nikam poznamenávať a sms s autorizačným kódom nesmie žiadnej osobe sprístupňovať.
6. Klient je povinný v závislosti od technického pokroku v oblasti funkcií mobilných zariadení zabezpečiť funkcie svojho mobilného zariadenia proti možnosti automatického pripojenia tretej osoby k mobilnému zariadeniu.
7. Pre smartbanking a autorizáciu využitím aplikácie smartbanking je najdôležitejšie mobilné zariadenie, na ktorom klient využíva aplikáciu smartbanking. Klient je povinný mať takéto mobilné zariadenie vždy pod dohľadom. Pre jeho zabezpečenie platia obdobne pravidlá pre mobilné zariadenia uvedené vyššie. Klient je povinný sa vždy odhlásiť z aplikácie smartbanking bezprostredne po ukončení práce s ňou a nikdy nepožičiavať ani neponechávať mimo dohľad svoje mobilné zariadenie, pokiaľ je prihlásený do aplikácie smartbanking.
8. Klient má povinnosť zabezpečiť na mobilnom zariadení, na ktorom sa rozhodne používať internetbanking alebo smartbanking, a kde je to technicky možné, aspoň antivírus a funkčný firewall a tieto ochranné prvky pravidelne aktualizovať. Banka odporúča, aby klient používal na mobilných zariadeniach, ktoré to umožňujú a prostredníctvom ktorých využíva služby Banky, aplikáciu smartbanking namiesto prihlasovania do internetbankingu prostredníctvom internetových prehliadačov.
9. I v prípade, že na mobilnom zariadení klient nepoužíva internetbanking ani smartbanking, ale v takomto mobilnom zariadení je zapojená SIM karta (tzn. SIM karta, ktorá obsahuje telefónne číslo, ktoré je určené k prijímaniu autorizačných sms kódov od Banky), je klient povinný zabezpečiť takéto mobilné zariadenie, pokiaľ je to technicky možné, aspoň funkčným firewallom a antivírovou ochranou a tieto ochranné prvky pravidelne aktualizovať.
10. Klient je povinný pravidelne sledovať informácie (najmä od Banky) o nových hrozbách, víroch, spywareoch apod. a v súlade s tým zaistiť ochranu mobilného zariadenia.
11. Postup uvedený v odsekoch 8 - 10 slúži k obmedzeniu rizika utajeného preposielania autorizačných sms kódov zasielaných Bankou (v prípade napadnutého mobilného zariadenia); alternatívou k obmedzeniu uvedeného rizika je používanie SIM karty výlučne v tzv. „hlúpych“ telefónoch.

## Čl. XIVa. Blokácia internetbankingu a smartbankingu

1. Banka je oprávnená trvalo alebo dočasne zablokovať internetbanking v prípade, že:
a) vznikne podozrenie na zneužitia internetbankingu alebo dôjde k zneužitiu internetbankingu,
b) sa významne zvýši riziko, že klient nebude schopný splácať úver, ktorý možno čerpať prostredníctvom internetbankingu.
2. Banka je oprávnená dočasne zablokovať internetbanking po určitom Bankou stanovenom počte neúspešných pokusov o prihlásenie do internetbankingu (napr. po piatich neúspešných pokusoch o prihlásenie, pričom v závislosti na počte neúspešných pokusov o prihlásenie je Banka oprávnená tento počet znížiť napr. aj na jeden neúspešný pokus). Banka je oprávnená stanoviť dobu dočasnej blokácie internetbankingu, pričom dĺžka dočasnej blokácie sa môže líšiť podľa počtu neúspešných pokusov o prihlásenie do internetbankingu (napr. dĺžka prvej dočasnej blokácie môže byť jedna hodina od neúspešného prihlásenia, dĺžka ďalšej dočasnej blokácie sa predĺži na dvojnásobok oproti dĺžke predchádzajúcej dočasnej blokácie, apod.).
3. Banka je oprávnená trvalo zablokovať internetbanking po určitom Bankou stanovenom počte po sebe idúcich dočasných blokácií (napr. siedmou po sebe idúcou dočasnou blokáciou môže dôjsť k trvalému zablokovaniu internetbankingu); v takom prípade je možné internetbanking odblokovať vydaním nového prvého hesla (na pobočke Banky či iným Bankou umožňovaným spôsobom).
4. Banka je oprávnená z bezpečnostných dôvodov dočasne či trvalo zablokovať internetbanking v prípade, že vznikne podozrenie, že telefónne číslo slúžiace na autorizáciu elektronicky

podaných pokynov nie je vo výhradnej dispozícii klienta, prípadne je oprávnená obmedziť internetbanking na jeho tzv. pasívnu podobu (bez možnosti autorizovať pokyny), prípadne iba znemožniť určitý spôsob autorizácie pokynov (napr. prostredníctvom autorizačných kódov zasielaných sms).

5. Banka je oprávnená trvalo alebo dočasne zablokovať smartbanking v prípade, že vznikne podozrenie zo zneužitia smartbankingu alebo dôjde k zneužitiu smartbankingu.
6. Banka je oprávnená trvalo alebo dočasne zablokovať použitie biometrického snímača pre aplikáciu smartbanking v mobilnom zariadení v prípade, že vznikne podozrenie zo zneužitia alebo dôjde ku zneužitiu tohto spôsobu autorizácie.
7. Pokiaľ Banka po zablokovaní internetbankingu, smartbankingu alebo použitia biometrického snímača pre aplikáciu smartbanking kontaktuje klienta, Banka ho kontaktuje Bankou zvoleným spôsobom (napríklad telefonicky, elektronicky či e-mailovou správou), a v takom prípade mu oznámi dôvody blokácie a dohodne s ním ďalší postup, napr. zmenu z dočasnej blokácie na trvalú blokáciu.

## Čl. XV. Kontaktujte klientskeho pracovníka

1. V prípade, že klient obdrží e-mail s upozornením na akúkoľvek zmenu v spôsobe prihlasovania do internetbankingu či s informáciou o zmene www adresy prihlasovacej stránky, alebo v prípade, že klient zistí netypické či inak podozrivé správanie sa prihlasovacej stránky, vrátane automatického presmerovania, alebo iné podozrivé skutočnosti, klient nesmie vykonávať žiadne úkony, ktoré by mohli viesť k prezradeniu či k zneužitiu dôverných údajov a je povinný bezodkladne kontaktovať pracovníkov Banky.
2. Klient má povinnosť informovať Banku pri podozrení z podvodu, pri podvode alebo pri bezpečnostnej hrozbe osobne na ktorejkoľvek pobočke Banky. Uvedeným postupom nie je dotknuté oznamovanie o zneužití internetbankingu a smartbankingu podľa čl. XVI. týchto podmienok.

## Čl. XVI. Oznámenie o zneužití internetbankingu a smartbankingu

1. Klient je povinný bezodkladne oznámiť Banke stratu, odcudzenie alebo zneužitie prihlasovacieho mena a hesla do internetbankingu či smartbankingu, neautorizovaný prístup do smartbankingu pomocou biometrických údajov, elektronického podpisu, mobilného zariadenia (SIM karty), na ktoré sa zasielajú sms kódy, mobilného zariadenia s aplikáciou smartbanking, tokenu pre služby API alebo iných dôverných údajov, ako aj iné zneužitie alebo neautorizované použitie internetbankingu či smartbankingu.
2. Klient je povinný oznámiť stratu, odcudzenie alebo zneužitie vyššie uvedených údajov a iné zneužitie či neautorizované použitie internetbankingu či smartbankingu telefonicky na tel. číslo: +421 2 2085 0310. Táto telefónna linka je klientovi k dispozícii nepretržite ktorýkoľvek deň v roku. Pri oznámení je klient povinný zodpovedať kontrolné otázky položené Bankou. Bez oznámenia týchto údajov sa nepovažuje oznámenie klienta za riadne a Banka nie je povinná takéto oznámenie prijať. Klient nesmie poskytnúť Banke svoje heslo pre prihlásenie do internetbankingu; Banka nebude od klienta požadovať poskytnutie hesla pre prihlásenie do internetbankingu. V prípade riadneho oznámenia je Banka oprávnená, ale nie povinná, overiť toto oznámenie napr. spätným kontaktovaním klienta. Klient súhlasí s tým, že Banka je oprávnená z preventívnych a bezpečnostných dôvodov od okamžiku riadneho prijatia oznámenia podľa tohto článku nevykonávať žiadne už podané alebo už prijaté pokyny na ťarchu účtu, ku ktorému má klient prístup na základe oznámeného prihlasovacieho mena do internetbankingu a zablokovať prístup do internetbankingu na základe tohto užívateľského mena. Banka nie je zodpovedná za škodu spôsobenú klientovi z dôvodu vykonania bezpečnostných opatrení podľa tohto článku.
3. Klient je povinný poskytnúť Banke všetku súčinnosť v súvislosti s oznámením o zneužití internetbankingu alebo smartbankingu vykonaného podľa tohto článku, a to najmä za účelom zistenia spôsobu či príčiny napadnutia zariadenia klienta. Klient je povinný zodpovedať na

otázky položené Bankou, ktoré podľa názoru Banky súvisia s oznámením klienta o možnom zneužití internetbankingu alebo smartbankingu. Klient je povinný na žiadosť Banky odovzdať zariadenie, prostredníctvom ktorého došlo (alebo mohlo dôjsť) k zneužitiu internetbankingu alebo smartbankingu alebo k vyzradeniu niektorých z informácii uvedených v odseku 1 tohto článku, príslušnému orgánu (najmä polícii) alebo Bankou zvolenému nestrannému odborníkovi za účelom preskúmania zariadenia. Z tohto dôvodu je klient povinný zdržať sa akýchkoľvek zásahov do zariadenia po zistení možného zneužitia internetbankingu alebo smartbankingu či možného vyzradenia niektorej informácie uvedenej v odseku 1 tohto článku. Banka odporúča klientovi pred odovzdaním zariadenia zálohovať celý (resp. pre klienta podstatný) obsah zariadenia.

## Čl. XVIa. Informácie o poskytovaní finančného sprostredkovania

1. Pri uzatváraní zmlúv a ďalších súvisiacich právnych úkonoch je Banka, pokiaľ z predmetného právneho úkonu nevyplýva inak, zastúpená obchodnou spoločnosťou Fio Slovakia, a.s., IČO: 35 828 137, so sídlom Nám. SNP 21, 811 01 Bratislava, zapísanou v obchodnom registri vedenom Okresným súdom Bratislava I., oddiel: Sa, vložka č.: 2892/B (ďalej aj len „finančný sprostredkovateľ“). Finančný sprostredkovateľ je akciovou spoločnosťou.
2. Finančný sprostredkovateľ je odo dňa 23.10.2015 pod registračným číslom 208336 zapísaný v Registri finančných agentov a finančných poradcov vedenom Národnou bankou Slovenska, dostupnom na webovej stránke https://regfap.nbs.sk/, ako viazaný finančný agent pre sektor poskytovania úverov a spotrebiteľských úverov a pre sektor prijímania vkladov a ako viazaný investičný agent pre sektor kapitálového trhu. Registráciu je možné overiť si na uvedenej webovej stránke.
3. Finančný sprostredkovateľ vykonáva finančné sprostredkovanie na základe písomnej mandátnej zmluvy výhradnej povahy, ktorú má uzatvorenú s jednou finančnou inštitúciou – Bankou. Finančný sprostredkovateľ je z titulu tejto zmluvy oprávnený zastupovať Banku pri uzatváraní zmluvy s klientom a k ďalším právnym úkonom v rámci zmluvného vzťahu s klientom. Odplatu za vykonávanie finančného sprostredkovania hradí Banka. Na žiadosť klienta bude jej výška oznámená. Finančný sprostredkovateľ vykonáva finančné sprostredkovanie v súlade s touto zmluvou a v súlade so zákonom č. 186/2009 Z.z. o finančnom sprostredkovaní a finančnom poradenstve a o zmene a doplnení niektorých zákonov.
4. Finančný sprostredkovateľ nemá kvalifikovanú účasť na základnom imaní ani hlasovacích právach Banky. Banka má kvalifikovanú účasť na základnom imaní a hlasovacích právach finančného sprostredkovateľa. Banka je jediným spoločníkom českej obchodnej spoločnosti RM-S FINANCE, s.r.o., IČO: 629 15 240 sídlo: Česká republika, 117 21 Praha 1, V Celnici 1028/10. Obchodná spoločnosť RM-S FINANCE, s.r.o. je jediným akcionárom finančného sprostredkovateľa.
5. Osobitnými predpismi upravujúcimi mimosúdne riešenie sporov vyplývajúcich z finančného sprostredkovania sú najmä zákon č. 244/2002 Z.z. o rozhodcovskom konaní, zákon č. 335/2014 Z.z. o spotrebiteľskom rozhodcovskom konaní a o zmene a doplnení niektorých zákonov, zákon č. 420/2004 Z.z. o mediácii a o doplnení niektorých zákonov a zákon č. 391/2015 Z.z. o alternatívnom riešení spotrebiteľských sporov a o zmene a doplnení niektorých zákonov.
6. Klient je oprávnený podať reklamáciu (sťažnosť) na vykonávanie finančného sprostredkovania Banke alebo finančnému sprostredkovateľovi v súlade s Reklamačným poriadkom Banky. Ďalšie podrobnosti sú uvedené v Reklamačnom poriadku zverejnenom na webovej stránke http://www.fio.sk.
7. Poplatky a iné náklady finančnej služby, ktoré hradí klient, sú uvedené v príslušnom Cenníku Banky. Finančnému sprostredkovateľovi klient Banky neplatí žiadnu odmenu.

## Čl. XVII. Záverečné ustanovenia

1. V záujme zlepšenia kvality služieb poskytovaných klientovi, v nadväznosti na vývoj právneho prostredia a tiež s ohľadom na obchodnú politiku Banky je Banka oprávnená tieto Podmienky meniť a dopĺňať (vyhlasovať nové znenie). Banka je oprávnená navrhnúť klientovi zmenu zmluvy o elektronickej správe účtu a týchto obchodných podmienok (vrátane Cenníka) (ďalej tiež „návrh na zmenu zmluvy“). Návrh na zmenu zmluvy sa klientovi poskytuje aspoň 2 mesiace pred navrhovaným dňom účinnosti zmeny, a to prostredníctvom internetbankingu, ak ho má klient zriadený, alebo na inom trvanlivom médiu. Zmluvné strany sa dohodli, že ak klient pred navrhovaným dňom účinnosti návrhu na zmenu zmluvy neoznámi Banke, že návrh na zmenu zmluvy neprijíma, platí, že klient návrh na zmenu zmluvy prijal. Ak klient nesúhlasí s návrhom na zmenu zmluvy, má právo na okamžité ukončenie zmluvy o elektronickej správe účtov bez poplatkov pred navrhovaným dňom účinnosti návrhu na zmenu zmluvy. Ak klient oznámi Banke, že s návrhom na zmenu zmluvy nesúhlasí, považuje sa to automaticky za výpoveď zmluvy o elektronickej správe účtov podanú Bankou, ak Banka nestanoví inak; v takom prípade sa za okamžik doručenia výpovede klientovi považuje doručenie (zo strany klienta) odmietnutia návrhu na zmenu Zmluvy a výpovedná lehota 2 mesiace začína plynúť nasledujúci deň. Oznámenie o nesúhlase klienta s návrhom na zmenu zmluvy, odvolanie tohto oznámenia, uplatnenie si práva na okamžité ukončenie zmluvy, ako aj prípadná výpoveď zmluvy zo strany klienta musia byť doručené Banke v písomnej podobe na adresu jej sídla či príslušnému pracovisku (pobočke). Ak bola podaná výpoveď zmluvy, klient je kedykoľvek pred dňom, kedy má navrhovaná zmena zmluvy nadobudnúť účinnosť, oprávnený odvolať svoj nesúhlas s návrhom na zmenu. Včasné odvolanie nesúhlasu s návrhom na zmenu zmluvy, podľa predchádzajúcej vety, má za následok, že automaticky podaná výpoveď zo strany Banky podľa predchádzajúcich ustanovení tohto odseku sa považuje za zrušenú (ak už neuplynula výpovedná lehota automaticky podanej výpovede). Klient žiada Banku, aby mu bol návrh na zmenu zmluvy alebo obchodných podmienok zaslaný prostredníctvom internetbankingu do tejto aplikácie v podobe nového úplného znenia zmluvy či obchodných podmienok tak, aby mohol tento návrh uchovať a využívať počas primeranej doby a aby mohol tento návrh v nezmenenej podobe reprodukovať. Banka žiadosť klienta prijíma.
2. Informácie o spracúvaní osobných údajov sú uvedené v Informačnom memorande Banky, ktorého aktuálne znenie je klientovi dostupné na webe https://www.fio.sk/o-nas/manualy-dokumenty-cenniky/informacne-materialy a taktiež na ktoromkoľvek klientskom pracovisku Banky.
3. Banka a klient sa dohodli, že Banka vyvinie snahu archivovať všetky informácie a dokumenty týkajúce sa i ukončeného zmluvného vzťahu medzi Bankou a klientom, a to za podmienky, že
   a) už v súlade s príslušnými postupmi nepristúpila ku skartácii daných dokumentov či informácií, a
   b) medzi Bankou a klientom existuje akýkoľvek ďalší zmluvný vzťah.
4. Banka sa zaväzuje postupovať podľa predchádzajúceho odseku tohto článku tak, aby podľa možnosti boli všetky dotknuté informácie a dokumenty skartované až naraz spolu s dokumentmi a informáciami vzťahujúcimi sa k poslednému zmluvnému vzťahu, u ktorého nie sú splnené podmienky pre ďalšiu archiváciu podľa predchádzajúceho odseku.
5. Pre účely predchádzajúcich dvoch odsekov tohto článku sa zmluvným vzťahom nerozumie taký zmluvný vzťah, na základe ktorého Banka poskytuje klientovi iba niektorú (či niektoré) z investičných služieb, investičných činnosti a vedľajších služieb v zmysle zákona o cenných papieroch (pre tieto účely vrátane prípadných úverov využívaných na účel umožnenia obchodu s finančným nástrojom).

6. Tieto Podmienky boli vyhlásené dňa 27. 10. 2022. Podmienky nadobúdajú účinnosť dňa 31. 10. 2022 a k rovnakému dňu nahrádzajú doterajšie Obchodné podmienky pre elektronickú správu účtov, ak nie je ďalej uvedené inak. Vo vzťahu k zmluvám uzatvoreným predo dňom účinnosti Podmienok podľa predchádzajúcej vety, nadobúdajú Podmienky účinnosť dňa 30. 12. 2022 a k rovnakému dňu nahrádzajú doterajšie Obchodné podmienky pre elektronickú správu účtov.

Ing. Marek Polka v. r.
vedúci organizačnej zložky