Obchodné podmienky
pre elektronickú správu účtov

vedených bankou **Fio banka, a.s.**, IČ: 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, Nám. SNP 21, 811 01 Bratislava, zapísanej v obchodnom registri vedenom Okresným súdom Bratislava I, oddiel: Po, vložka č.: 1875/B (ďalej aj len „Banka“)

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., IČ: 61858374, ČR (ďalej tiež len „internetbanking“). 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. Súčasne určí majiteľ účtu aj rozsah splnomocnenia, tzn. určí, ktoré úkony je splnomocnená osoba oprávnená vykonávať. Splnomocnená osoba spravuje účet majiteľa v medziach splnomocnenia svojím vlastným prihlasovacím menom, heslom a zvoleným spôsobom autorizácie elektronickej komunikácie.
2. Tieto obchodné podmienky pre elektronickú správu účtov (ďalej tiež len 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.

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 Banky a počítačom či obdobným mobilným zariadením, ako napríklad tzv. chytrým telefónom, (ďalej len „počítač“) klienta buď prostredníctvom dátových alebo telefónnych liniek. Adresa serveru Banky je: www.fio.sk, ib.fio.sk. Za adresu serveru Banky sa však považuje aj: www.fio.cz, ib.fio.cz. Banka má právo kedykoľvek obmedziť prístup na ktorýkoľvek zo serverov banky, a to dočasne i trvalo.
2. Klient je pri každom svojom pripojení na server Banky povinný overiť jeho identifikáciu (SHA1 Fingerprint) porovnaním s touto správnou identifikáciou: B0:DF:13:F6:59:8B:D5:C3:95:CD:CE:09:03:C5:CF:D0:D6:4E:0C:95 (v Microsoft Internet Explorer je toto číslo zobrazované bez oddeľujúcich dvojbodiek). Banka nezodpovedá za škodu spôsobenú porušením tejto povinnosti klientom. Identifikáciu servera Banky overíte v okne, ktoré otvoríte kliknutím na ikonu „žltého visiaceho zámku“, ktorá je, v závislosti od použitého internetového prehliadača, umiestnená obvykle na hornej alebo dolnej ovládacej lište. 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.

2a. Klient je pri každom svojom pripojení aplikáciou Fio-podpis (ďalej tiež len „elektronický kľúč“) povinný overiť jej identifikáciu (SHA1 Fingerprint) porovnaním s touto správnou identifikáciou: B7:7B:9E:D2:1F:C8:B3:0C:12:DA:0A:5E:13:53:26:7B:F2:8D:70:D7, po aktualizácii certifikátu s touto správnou identifikáciou: 2A:3C:95:42:AB:AA:56:26:78:AD:8A:2C:67:89:D6:F8:EC:BC:69:8A. Banka nezodpovedá za škodu spôsobenú porušením tejto povinnosti klientom. Identifikáciu 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.

3. Identifikácia podľa ods. 2 a 2a je pravidelne menená. O tejto zmene je klient informovaný v dostatočnom predstihu oznámením na stránkach serveru Banky. Súčasne sú zmenené tieto Podmienky. Ak dôjde k zmene identifikácie, je klient povinný pri svojom najbližšom pripojení na server Banky overiť novú identifikáciu. Jej správne znenie získa na ktorejkoľvek pobočke Banky a v týchto Podmienkach. Banka nezodpovedá za škodu spôsobenú porušením tejto povinnosti klientom.

4. 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.

III. Autorizácia elektronicky zadaných pokynov

1. Elektronicky podané pokyny musia byť klientom autorizované, tzn. podpísané jedným z nižšie uvedených spôsobov alebo ich kombináciou, v závislosti od spôsobu zvoleného klientom, prípadne stanoveného Bankou v čl. VII Podmienok. Pokyny podané elektronicky pomocou smartbankingu musia byť klientom autorizované zadaním PINu pre smartbanking, pričom tento spôsob autorizácie nie je možné kombinovať s ostatným spôsobmi. Aplikácia smartbanking môže na niektorých mobilných zariadeniach umožniť nahradenie PINu pre smarbanking alebo prístupových údajov pre smartbanking (vždy však maximálne jedného z týchto bezpečnostných prvkov) použitím zabudovaného biometrického snímača. Ak bol pokyn autorizovaný, má sa za to, že klient súhlasil s podaním a vykonaním pokynu, ak klientom nie je preukázané, že pokyn neautorizoval.

2. **Autorizácia elektronickým podpisom**. Banka dodá klientovi program, ktorý mu umožní vytvoriť si vlastný elektronický podpis – šifrovací kľúč. Verejnú časť svojho šifrovacieho kľúča odovzdá klient osobne Banke pred spustením elektronickej komunikácie. Správa prístupu k tajnej časti šifrovacieho 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 šifrovací 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 uvedením svojho hesla k súkromnej časti elektronického Fio – podpisu (šifrovacieho kľúča) do príslušného poľa formulára pre zadávanie pokynov v rámci internetbankingu po tom, čo sa riadne prihlásil do internetbankingu svojím prihlasovacím menom a prístupovým heslom. Následne je vygenerovaná verejná časť elektronického Fio– podpisu, ktorá je zaslaná Banke. Banka overí zhodu zaslanej verejnej časti elektronického Fio – podpisu s verejnou časťou elektronického Fio – podpisu, ktorá bola uložená u Banky. Ak je zaslaná a uložená verejná časť elektronického Fio – podpisu zhodná, je pokyn autorizovaný.

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. 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 svojím prihlasovacím menom a prístupovým heslom. Ak je klientom vložený sms kód zhodný s sms kódom vygenerovaným a zaslaným Bankou, je pokyn autorizovaný.

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 používanie smartbankingu pokynom v internetovom rozhraní internetbankingu spoločne so zadaním prístupového hesla smartbankingu a zadaním unikátneho identifikačného kódu (ďalej len „UID“) mobilného zariadenia, ktoré bude pre prístup k smartbankingu používané (pričom z iného mobilného zariadenia nebude prístup umožnený). Tento pokyn musí byť riadne autorizovaný elektronickým podpisom a/alebo jednorazovým sms kódom, v závislosti od spôsobu autorizácie zvolenej klientom. Ak bude chcieť klient prostredníctvom smartbankingu podávať pokyny, je nevyhnutné zriadiť v internetovom rozhraní internetbankingu PIN pre smartbanking a tento PIN riadne autorizovať elektronickým podpisom a/alebo jednorazovým sms kódom, v závislosti od spôsobu autorizácie zvolenej klientom. Autorizáciu pokynu prostredníctvom PINu pre smartbanking vykonáva klient zadaním PINu pre smartbanking do príslušného pola pre zadávanie pokynov v aplikácii smartbanking po tom, čo sa riadne prihlásil do smartbankingu svojím prihlasovacím menom a heslom smartbankingu.

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 (vždy však maximálne jedného z týchto bezpečnostných prvkov) použitím zabudovaného 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 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 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 prostredníctvom internetového rozhrania internetbankingu (resp. okamihom nastavenia použitia biometrického snímača podľa ods. 3b), i keď tento spôsob autorizácie nie je uvedený 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. 3a môže klient meniť

elektronicky prostredníctvom internetového rozhrania internetbankingu. Spôsob a podmienky autorizácie podľa ods. 3b môže klient zmeniť elektronicky prostredníctvom aplikácie smartbanking.

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.), aj keď neboli založené pomocou elektronickej správy účtov, pokiaľ sa Banka a klient nedohodnú inak. Po dobu jedného roka odo dňa zrušenia účtu môže klient naďalej získavať všetky informácie o účte či podúčte, vrátane pohybov na účte či podúčte.

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. XVa 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 XVa týchto podmienok, najmä porušenie opatrení za účelom zaistenia bezpečnosti a utajenia dôverných údajov, porušenie povinností na zabezpečenie počítača používaného pre prístup do internetbankingu, porušenie povinností na zabezpečenie mobilného zariadenia/SIM karty používanej na zasielanie SMS kódov, porušenie povinnosti overiť identifikáciu servera Banky alebo aplikácie pre elektronický podpis alebo porušenie povinnosti včas oznámiť Banke podozrenie na zneužitie bezpečnostných údajov.
4. Klient neznáša nijaké finančné dôsledky vyplývajúce zo zneužitia internetbankingu od okamihu oznámenia skutočnosti podľa článku XVa okrem prípadov, keď konal podvodným spôsobom.
5. Klient znáša stratu až do 100 eur, ktorá súvisí so všetkými neautorizovanými platobnými operáciami vykonanými prostredníctvom internetbankingu a ktorá je spôsobená zneužitím internetbankingu neoprávnenou osobou v dôsledku nedbanlivosti klienta pri zabezpečovaní dôverných údajov, t.j. v dôsledku nedbanlivosti pri plnení povinnosti klienta vykonať všetky primerané úkony na zabezpečenia dôverných údajov (ako personalizovaných bezpečnostných prvkov internetbankingu), ak v zmluve či Podmienkach nie je uvedené inak. 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 z dôvodu poruchy prenosovej siete alebo z dôvodu náhody, t.j. nepredvídateľnej a na vôli Banky nezávislej udalosti, ktorej následky nemohla Banka odvrátiť.

7. Banka zodpovedá za nesprávne vykonanie pokynu, ibaže klientovi doloží, že čiastka nesprávne vykonaného pokynu bola riadne a včas pripísaná na účet poskytovateľa platobných služieb príjemcu.
8. Banka nezodpovedá za platobnú operáciu vykonanú na základe neautorizovaného pokynu alebo za chybne vykonanú platobnú operáciu, ak klient neoznámil túto skutočnosť Banke bez zbytočného odkladu odo dňa zistenia neautorizovanej alebo chybne vykonanej platobnej operácie, najneskôr však do 13 mesiacov odo dňa odpísania peňažných prostriedkov, z príslušného účtu.¨

VI. Zmluvná odmena a poplatky

1. Výška odmeny účtovaná Bankou za umožnenie elektronické správy účtov je uvedená v Cenníku finančných operácií a služieb, 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.

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

1. Ak je príslušná služba Bankou poskytovaná a ak nie je ďalej uvedené inak, elektronickou správou účtov 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,
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 informačného hlásiča 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,
r) voľba použitia biometrického snímača v mobilnom zariadení pre smartbanking (toto možno nastaviť iba cez smartbanking)

2. 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) prehľad podaných pokynov spolu s ich stavmi.

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

3. Niektoré pokyny podľa ods. 1, podľa požiadaviek Banky týkajúcich sa autorizácie a aktuálnych v čase zadávania pokynu, musia byť autorizované podľa čl. III. Podmienok. Niektoré z pokynov a informácií, ktoré možno podávať resp. získavať prostredníctvom el. správy účtov, uvádzané v ods. 1 a 2, môžu byť pri použití smartbankingu obmedzené v závislosti od verzie aplikácie, mobilného zariadenia či jeho operačného systému.
4. Elektronickou správou účtov je možné zadať požiadavku na založenie alebo zrušenie informačného hlásiča o niektorých udalostiach na účte. Klient si môže zvoliť hlásič 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.

VIII. Bezpečnostné upozornenia súvisiace s využívaním internetbankingu

1. V súvislosti s využívaním elektronických komunikačných služieb si Vás dovoľujeme informovať o niektorých bezpečnostných rizikách s tým spojených a upozorniť Vás na základné možnosti, ktorými môžete Vy, 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, telefónne číslo, UID mobilného zariadenia, kód (passcode, PIN) pre prístup k mobilnému zariadeniu a iné dôverné alebo citlivé údaje (ďalej tiež „dôverné údaje“) a počítač pred ich zneužitím. Ide o základné pravidlá, ktoré je potrebné dodržiavať na ochranu Vašich dôverných údajov a Vášho počítača.
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 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.

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 počítača klienta, ktorý je používaný pre prihlásenie do internetbankingu 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, počítača klienta alebo v dôsledku nesprávneho nakladania s týmito údajmi klientom, pokiaľ nejde o prípad porušenia povinností na strane Banky.

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 do internetbankingu), ktoré sú prenášané medzi počítačom klienta a serverom Banky. Všetky dáta sú šifrované štandardom SSL 128bit. 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 súvisiacich s využívaním internetbankingu sú uvedené tiež na tejto webovej adrese: http://www.fio.sk/bankove-sluzby/internetbanking.

XI. Utajení dôverných údajov

1. Chráňte svoje dôverné údaje pred zverejnením a zneužitím.
2. Dôverné údaje si nezaznamenávajte. Ak si dôverné údaje napriek tomu poznamenáte, uschovajte ich na mieste, ktoré nie je voľne prístupné tretím osobám.
3. Neuvádzajte 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 počítačom).
4. Nezadávajte dôverné údaje pred inou osobou, neposkytujte dôverné údaje iným osobám, a to ani rodinným príslušníkom a blízkym osobám.
5. Vaše heslo stanovte najlepšie ako kombináciu čísiel a veľkých a malých písmen, bez osobného vzťahu k Vám či k blízkym osobám. Jednoduché heslo s osobnými rysmi je ľahšie odhaliteľné. Ako heslo a PIN pre smartbanking nepoužívajte svoj dátum narodenia, rodné číslo, telefónne číslo, po sebe idúce číslice apod. Heslo a PIN pre smartbanking pravidelne meňte. Nikdy nemeňte heslo do internetbankingu na inom formulári, než v záložke Globálne nastavenia v internetbankingu. Banka od Vás v žiadnom prípade nebude vyžadovať iný postup. Prvé heslo musíte zmeniť pri prvom prihlásení do internetbankingu. Platnosť nasledujúceho hesla je z bezpečnostných dôvodov obmedzená na 365 dní. Ak vyprší uvedené lehota, budete pri najbližšom prihlásení do internetbankingu vyzvaní k zmene hesla.
6. Neposielajte dôverné údaje pomocou e-mailu alebo sms, nezadávajte ich na inej internetovej stránke, než na stránke určenej na prihlasovanie do internetbankingu, a to ani v prípade, ak obdržíte e-mail či sms , ktorá napodobňuje výzvu, najmä od Banky, na zaslanie dôverných údajov alebo na ich vyplnenie na inej internetovej stránke. Banka Vám takýto druh správ v žiadnom prípade nebude posielať.

XII. Uloženie elektronického kľúča

1. Chráňte svoj elektronický kľúč, ktorý používate pri zadávaní pokynov, proti jeho zneužitiu, najmä proti jeho odcudzeniu, skopírovaniu a pod. Zneužitím Vášho elektronického kľúča

môže iná osoba predstierať Vašu identitu a zadávať pokyny Vaším menom. Zneužitie elektronického kľúča Vám môže spôsobiť škodu.
2. Elektronický kľúč inštalujte iba na počítač, o ktorom viete, že je chránený pred možnými hrozbami plynúcimi z pripojenia k dátovej sieti. Neinštalujte a nepoužívajte kľúč na počítač, ktorý je verejne prístupný.
3. Ak uchovávate elektronický kľúč na inom prenosnom médiu, uložte toto médium na miesto, kde nedôjde k jeho zneužitiu, najmä odcudzeniu, skopírovaniu či poškodeniu.

XIII. Preventívne opatrenia vo sfére vplyvu klienta, zabezpečenie počítača klienta

1. Internetbanking používajte iba na počítačoch, ktoré sú riadne zabezpečené proti zneužitiu dôverných údajov.

Nepoužívajte internetbanking hlavne v internetových kaviarňach a na iných verejne prístupných počítačoch, ani na počítačoch, u ktorých nemáte istotu, že sú zabezpečené proti zneužitiu dôverných údajov.

2. Pred prihlásením do internetbankingu sa riadne presvedčte, že komunikujete so správnym poskytovateľom služby. Adresa servera Banky je www.fio.sk, ib.fio.sk. (resp. tiež www.fio.cz, ib.fio.cz). Banka má právo kedykoľvek obmedziť prístup na ktorúkoľvek z uvedených adries, a to dočasne i trvalo. Pri prihlasovaní do aplikácie internetbanking a pri zadávaní pokynov prostredníctvom aplikácie internetbanking riadne skontrolujte, že spojenie je zabezpečené (overte platnosť certifikátu SSL zabezpečenia) a ďalej overte identifikáciu servera Banky. V prípade pochybností o tom, že komunikujete s Bankou, alebo že spojenie nie je riadne zabezpečené, nevykonávajte žiadne úkony, ktoré by mohli viesť k prezradeniu alebo zneužití dôverných údajov a bezodkladne kontaktujte klientskeho pracovníka Banky.
3. Počítač, na ktorom sa rozhodnete používať internetbanking, zabezpečte legálnym firewallom, antivírovou a anti- spyware ochranou, a tieto ochranné prvky pravidelne aktualizujte. Programy aktualizujte štandardným spôsobom. Pravidelne sledujte informácie o nových hrozbách, vírusoch, spyware a pod. a v súlade s tým zabezpečte ochranu Vášho počítača.
4. Používajte legálny a pravidelne aktualizovaný operační systém vo Vašom počítači. Pravidelne sledujte správy výrobcu Vášho operačného systému o opravách chýb a nedostatkov tohto operačného systému a tieto opravy

včas inštalujte do Vášho počítača.

5. Ak používate internetbanking na určitom počítači, vyvarujte sa sťahovaniu a inštalovaniu programov, ktoré možno voľne získať na internete, u ktorých si nie ste istí, či neobsahujú vírusy alebo spyware, prípadne nepochádzajú zo zdroja, ktorý je dôveryhodný. Navštevujte iba známe, dôveryhodné a bezpečné stránky na internete. Neotvárajte nevyžiadané emaily, emaily od neznámych odosielateľov a emaily s podozrivým názvom alebo obsahom na takomto počítači. Takéto emaily bez otvorenia zmažte. Vo svojej emailovej schránke používajte spam filter.
6. Žiadne licenčné podmienky pri voľne šírenom software Vám nemôžu poskytnúť istotu, že software neobsahuje súčasti, ktoré môžu Váš počítač poškodiť či inak narušiť bezpečnosť Vami ukladaných údajov.
7. Pre získanie základných informácií o možnostiach zabezpečenia Vášho počítača a o rizikách, ktoré hrozia Vášmu počítaču, si prosím prečítajte informácie na stránkach www.microsoft.com/cze/athome/security/protect/.

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“). Túto SIM kartu majte vždy pod dohľadom, mobilné zariadenie bez SIM karty neumožní komunikáciu s Bankou a autorizáciu..
2. Mobilné zariadenie či s SIM kartu neponechávajte ležať na miestach, kde nad nimi nemáte kontrolu.

3. Vyvarujte sa požičiavaniu mobilného zariadenia či SIM karty tretím osobám bez toho, aby ste mali neustálu kontrolu nad ich nakladaním s mobilným zariadením a SIM kartou.
4. V prípade, že hrozí riziko, že by ste mohli ponechať mobilné zariadenie mimo Váš dohľad, znemožnite jeho používanie tretím osobám kódom PIN. Tento kód uchovávajte v tajnosti a neoznamujte ho tretím osobám, ani si ho nikam nepoznamenávajte.
5. Autorizačný kód, ktorý Vám je doručený Bankou, si nikam nepoznamenávajte a sms s autorizačným kódom žiadnej osobe nesprístupňujte.
6. V závislosti od technického pokroku v oblasti funkcií mobilných zariadení zabezpečte funkcie svojho mobilného zariadenia proti možnosti automatického pripojenia tretej osoby k Vášmu mobilnému zariadeniu.
7. Pre smartbanking a autorizáciu využitím aplikácie smartbanking je najdôležitejšie mobilné zariadenie, ktorého UID ste určili pre tento druh služby. Toto mobilné zariadenie majte vždy pod dohľadom, pre jeho zabezpečenie platia obdobne pravidlá pre mobilné zariadenia uvedené vyššie. Vždy sa odhláste z aplikácie smartbanking bezprostredne po ukončení práce s ňou a nikdy nepožičiavajte ani neponechávajte mimo dohľad svoje mobilné zariadenie, ak ste prihlásení do aplikácie smartbanking.

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 trvalo alebo dočasne zablokovať smartbanking v prípade, že vznikne podozrenie zo zneužitia smartbankingu alebo dôjde k zneužitiu smartbankingu.
3. Banka je oprávnená trvalo alebo dočasne zablokovať použitie biometrického snímača pre aplikáciu smartbanking v mobilnom zariadení v prípade, že vznikne podozrenie zo zneužitia tohto spôsobu autorizácie.

XV. Kontaktujte klientskeho pracovníka

1. V prípade, že obdržíte 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 zistíte netypické či inak podozrivé správanie sa prihlasovacej stránky, vrátane automatického presmerovania, alebo iné podozrivé skutočnosti, nevykonávajte žiadne úkony, ktoré by mohli viesť k prezradeniu či k zneužitiu dôverných údajov a bezodkladne informujte klientskych pracovníkov Banky a vyžiadajte si radu ohľadne ďalšieho postupu.

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 alebo iných dôverných údajov, ako aj iné zneužitie alebo neautorizované použitie internetbankingu či smartbankingu.
2. Klient oznámi stratu, odcudzenie alebo zneužitie vyššie uvedených údajov a iné zneužitie či neautorizované použitie internetbankingu či smartbankingu telefonicky na tel. číslo: +421 2 5262 0990. Táto telefónna linka je klientovi k dispozícii nepretržite ktorýkoľvek deň v roku. Pri oznámení je klient povinný uviesť aspoň tieto údaje: osobné identifikačné údaje a svoje prihlasovacie meno do internetbankingu. Bez oznámenia týchto údajov sa nepovažuje oznámenie klienta za riadne a Banka nie je povinná takéto oznámenie prijať. 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.

XVII. Záverečné ustanovenia

1. V záujme zlepšenia kvality služieb poskytovaných klientovi, v súvislosti so zmenou identifikácie (fingerprintu) serveru Banky, v nadväznosti na vývoj právneho prostredia a tiež s ohľadom na obchodnú politiku Banky je Banka oprávnené tieto Podmienky meniť a dopĺňať (vyhlasovať nové znenie). Banka je oprávnená navrhnúť klientovi zmenu zmluvy o elektronickej správe účtu a týchto obchodných podmienok (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. 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. 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 oprávnený pred uplynutím výpovednej doby a pred navrhovaným dňom účinnosti návrhu na zmenu zmluvy odvolať svoj nesúhlas s návrhom na zmenu. Včasné odvolanie nesúhlasu s návrhom na zmenu zmluvy, podľa predchádzajúcej vety, má za následok, že podaná výpoveď sa považuje za zrušenú. 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. Tieto Podmienky boli vyhlásené dňa 21.4.2015, nadobúdajú účinnosť dňa 22.6.2015 a nadobudnutím účinnosti nahrádzajú predchádzajúcu verziu „Obchodných podmienok pre elektronickú správu účtov“ vedených bankou Fio banka, a.s. (prostredníctvom organizačnej zložky Fio banka, a.s., pobočka zahraničnej banky).

Ing. Marek Polka
v. r. vedúci
organizačnej zložky