Obchodní podmínky pro elektronickou správu účtů

vedených bankou **Fio banka, a.s.,**
IČ 61858374, Praha 1, V Celnici 10, PSČ 117 21,
zapsanou v obchodním rejstříku vedeném rejstříkovým soudem v Praze, spis. zn. B, vložka 2704

Čl. I. Předmět úpravy

1. Fio banka, a.s. (dále jen banka) umožňuje svým klientům na základě uzavřené smlouvy o elektronické správě účtů (dále jen „smlouva“) elektronicky spravovat jejich účty u ní vedené (dále také „internetbanking“). Píše-li se dále o internetbankingu, může tím být dle povahy úpravy myšlen též tzv. „smartbanking“, tedy služba přímého bankovnictví, za pomocí niž banka umožňuje svým klientům spravovat jejich účty u ní vedené, a to za použití k tomu bankou určené aplikace smartbanking v klientově mobilním zařízení. Pro smartbanking platí všechna následující ustanovení stejně tak jako pro internetbanking, není-li dále uvedeno jinak. Elektronickou správou účtů se rozumí bezdokladové elektronické podávání pokynů a provádění dalších služeb poskytovaných k účtu a získávání informací o účtu a provedených službách. Oprávnění k elektronické správě účtu fyzické osoby může udělit majitel účtu elektronicky ve prospěch třetí fyzické osoby - klienta banky určením jeho přihlašovacího jména a přiděleného čísla klienta banky. Oprávnění k elektronické správě účtu právnické osoby může udělit písemně osoba oprávněná jednat za právnickou osobu ve prospěch třetí fyzické osoby. Současně určí majitel účtu i rozsah zmocnění, tj. které úkony je zmocněná osoba oprávněna činit. Zmocněná osoba spravuje účet majitele v mezích zmocnění přiděleným číslem klienta pro přihlášení do elektronické správy účtů, heslem a zvoleným způsobem autorizace elektronické komunikace.
2. Tyto Obchodní podmínky pro elektronickou správu účtů (dále jen „Podmínky“) doplňují či podrobněji upravují některá ustanovení smlouvy, případně k nim činí závazný výklad. V případě rozporu mezi úpravou ve smlouvě a Podmínkách platí ustanovení smlouvy.

Čl. II. Způsob přenosu a zabezpečení přenášených dat

1. Všechny pokyny a informace, které lze podat, resp. získat pomocí elektronické správy účtů jsou přenášeny mezi serverem Fio banky, a.s. a počítačem či obdobným mobilním zařízením jako například tzv. chytrým telefonem (dále jen počítač) klienta buď prostřednictvím datových nebo telefonních linek. Adresa serveru banky je: http://www.fio.cz/.
2. Klient je při každém svém připojení na server banky povinen ověřit jeho identifikaci (SHA1 Fingerprint) porovnáním s touto správnou identifikací: 92:DB:4B:00:79:C2:1E:FA:C5:63:33:4D:C5:0C:E6:0D:8A:F4:B7:05, po aktualizaci certifikátu s touto správnou identifikací: D2:31:FA:DA:0D:78:E0:73:31:C4:1C:E7:AB:89:64:9E:25:46:40:E6 (v Microsoft Internet Exploreru je toto číslo zobrazováno bez oddělujících dvojteček). Banka neodpovídá za škodu způsobenou porušením této povinnosti klientem. Identifikaci serveru banky ověříte v okně, které otevřete kliknutím na „žlutou ikonu visacího zámku“, která je umístěna na stránce pro přihlášení do internetbankingu. Tato ikona bývá umístěna obvykle např. na horní nebo dolní ovládací liště v závislosti na použitém webovém prohlížeči. V případě aplikace smartbanking je klient povinen ověřit identitu poskytovatele a autora aplikace při její instalaci do mobilního zařízení, při připojení na server banky prostřednictvím aplikace smartbanking již klient ověření identifikace serveru banky neprovádí.

2a. Klient je při každém svém připojení aplikací Fio-podpis (dále také „elektronický klíč“) povinen ověřit její identifikaci (SHA1 Fingerprint) porovnáním s touto správnou identifikací: B7:7B:9E:D2:1F:C8:B3:0C:12:DA:0A:5E:13:53:26:7B:F2:8D:70:D7, po aktualizaci certifikátu s touto správnou identifikací: 2A:3C:95:42:AB:AA:56:26:78:AD:8A:2C:67:89:D6:F8:EC:BC:69:8A. Banka neodpovídá za škodu způsobenou porušením této povinnosti klientem. Identifikace Fio-podpisu je zobrazena v okně prostředí JAVA při spouštění aplikace Fio podpis, nebo - v případě přijetí tohoto certifikátu za důvěryhodný - v důvěryhodných certifikátech v prostředí JAVA.

3. Identifikace dle odst. 2 a 2a je pravidelně měněna. O této změně je klient informován v dostatečném předstihu oznámením na stránkách serveru banky. Současně jsou změněny tyto Podmínky. Jestliže dojde ke změně identifikace, je klient povinen při svém nejbližším připojení na server banky ověřit novou identifikaci. Její správné znění získá na kterékoliv pobočce banky a v těchto Podmínkách. Banka neodpovídá za škodu způsobenou porušením této povinnosti klientem.
4. Banka zřizuje klientovi přístup na neveřejné stránky serveru banky pomocí uživatelského jména a hesla, které si klient zvolí a dohodnutým způsobem předá bance. Klient je oprávněn heslo kdykoliv změnit.

Čl. III. Autorizace elektronicky podaných pokynů

1. Elektronicky podané pokyny musí být klientem autorizovány, tj. podepsány jedním z dále uvedených způsobů, nebo jejich kombinací, v závislosti na způsobu zvoleném klientem, případně stanoveném bankou v čl. VII Podmínek. Elektronicky podané pokyny za pomoci smartbankingu musí být klientem autorizovány zadáním PINu pro smartbanking, přičemž tento způsob autorizace nelze kombinovat s ostatními způsoby. Jestliže byl pokyn autorizován, má se za to, že klient souhlasil s podáním a provedením pokynu, pokud není klientem prokázáno, že pokyn neautorizoval.
2. Autorizace elektronickým podpisem. Banka dodá klientovi program, který mu umožní vytvořit si vlastní elektronický podpis – šifrovací klíč. Klient je oprávněn po započetí elektronické komunikace změnit šifrovací klíč. Změnu šifrovacího klíče provede klient tak, že v programu dodaného mu bankou si vytvoří nový šifrovací klíč, jehož veřejnou část zašle bance pokynem prostřednictvím internetbankingu nebo jej osobně předá na její pobočce. V případech, kdy banka prostřednictvím internetbankingu vyzve klienta ke změně šifrovacího klíče, je klient povinen tuto změnu provést ve lhůtě uvedené ve výzvě. V opačném případě banka šifrovací klíč po marném uplynutí lhůty zruší. Po zrušení šifrovacího klíče nebude klient moci provádět pokyny, které vyžadují autorizaci dle čl. VII odst. 3 Podmínek, a to do doby, dokud neprovede změnu šifrovacího klíče výše uvedeným způsobem. Veřejnou část svého šifrovacího klíče předá klient osobně před započetím elektronické komunikace bance. Správa přístupu k tajné části šifrovacího klíče a heslu klíče je plně v odpovědnosti klienta. Je-li klientem právnická osoba, musí každá fyzická osoba, která je oprávněna jménem klienta podávat pokyny a získávat informace, mít své uživatelské jméno a heslo, které je považováno za uživatelské jméno a heslo klienta, a svůj šifrovací klíč. Manuál pro elektronickou aplikaci Fio-podpis určený pro instalaci a použití elektronického podpisu je možné získat na každé pobočce banky nebo ho lze získat na webové stránce banky: http://www.fio.cz/spolecnost-fio/manualy-dokumenty-ceniky/manualy. Klient je povinen při instalaci a použití elektronického Fio - podpisu postupovat podle uvedeného manuálu. Autorizaci pokynu prostřednictvím elektronického

Fio - podpisu provádí klient uvedením svého hesla k soukromé části elektronického Fio – podpisu (šifrovacího klíče) do příslušného pole formuláře pro zadávání pokynů v rámci internetbankingu poté, co se řádně přihlásil do internetbankingu svým přihlašovacím jménem a přístupovým heslem. Následně je vygenerována veřejná část elektronického Fio – podpisu, která je zaslána bance. Banka ověří shodu zaslané veřejné části elektronického Fio – podpisu s veřejnou částí elektronického Fio – podpisu, která byla uložena u banky. Je-li zaslaná a uložená veřejná část elektronického Fio – podpisu shodná, je pokyn autorizován.

3. Autorizace jednorázovým sms kódem. Klient sdělí bance telefonické číslo, na které bude banka klientovi zasílat sms zprávy s jednorázovým autorizačním kódem. Autorizační kód je určen vždy k jednoznačně definovanému pokynu. Klient si v rámci nastavení podmínek autorizace může zvolit délku autorizačního kódu (5 – 25 znaků), počet pokusů pro zadání kódu (1- 5 pokusů) a platnost autorizačního kódu (max. 20 minut). V případě propadnutí platnosti autorizačního kódu (vygenerování nového autorizačního kódu k zadanému pokynu, uplynutí stanovené doby platnosti) klient může požádat o zaslání nového jednorázového autorizačního kódu. Autorizaci pokynu prostřednictvím sms kódu provádí klient uvedením zaslaného sms kódu do příslušného pole formuláře pro zadávání pokynů v rámci internetbankingu poté, co se řádně přihlásil do internetbankingu svým přihlašovacím jménem a přístupovým heslem. Je-li klientem vložený sms kód shodný s sms kódem vygerovaným a zaslaným bankou, je pokyn autorizován.

3a. Autorizace PINem pro smartbanking. Pro používání smartbankingu si klient do svého mobilního zařízení opatří bankou určenou aplikaci smartbanking umožňující poskytování této služby dle operačního systému mobilního zařízení (na internetových stránkách banky lze najít odkazy na autorizované zdroje této aplikace). Bankou určenými aplikacemi smartbanking nemusí být podporovány všechny typy mobilních zařízení a jejich operační systémy. Klient zřídí používání smartbankingu pokynem v internetovém rozhraní internetbankingu společně se zadáním přístupového hesla smartbankingu a zadáním unikátního identifikačního kódu (dále jen „UID“) mobilního zařízení, kterého bude pro přístup k smartbankingu používáno (přičemž z jiného mobilního zařízení nebude přístup umožněn). Tento pokyn musí být řádně autorizován elektronickým podpisem a/nebo jednorázovým sms kódem v závislosti na způsobu autorizace zvolené klientem. V případě, že bude chtít klient prostřednictvím smartbankingu podávat pokyny, je nezbytné v internetovém rozhraní internetbankingu zřízení PINu pro smartbanking a jeho řádná autorizace elektronickým podpisem a/nebo jednorázovým sms kódem v závislosti na způsobu autorizace zvolené klientem. Autorizaci pokynu prostřednictvím PINu pro smartbanking provádí klient zadáním PINu pro smartbanking do příslušného pole pro zadávání pokynů v aplikaci smartbanking poté, co se řádně přihlásil do smartbankingu svým přihlašovacím jménem a heslem smartbankingu.

4. Nastavení způsobu a podmínek autorizace dle odst. 2 a odst. 3 konkrétního klienta je uvedeno v Protokolu o nastavení autorizace el. pokynů. Nastavení způsobu a podmínek autorizace PINem pro smartbanking dle odst. 3a je považováno za nastavenou autorizaci elektronických pokynů podle Smlouvy o elektronické správě účtů okamžikem zřízení smartbankingu klientem prostřednictvím internetového rozhraní internetbankingu, i když tento způsob autorizace není uveden v Protokolu o nastavení autorizace elektronických pokynů.

5. Způsob a podmínky autorizace dle odst. 2 a odst. 3 může klient změnit osobně na pobočce banky. Způsob a podmínky autorizace dle odst. 3a může klient změnit elektronicky prostřednictvím internetového rozhraní internetbankingu.

Čl. IV. Zřizování a rušení podúčtů běžného účtu a rušení účtů pomocí elektronické správy

1. Prostřednictvím elektronické správy účtů lze zřizovat a rušit podúčty běžného účtu (dále jen podúčty), je-li to výslovně uvedeno jako jedna z možností v čl. VIII.
2. Prostřednictvím elektronické správy účtů lze též rušit účty, s výjimkou běžných účtů, Fiokonta, běžných vkladů, speciálních běžných účtů a účtů, o nichž to stanoví smlouva či Obchodní podmínky pro zřizování a vedení účtů (dále jen „obchodní podmínky“), i když nebyly založeny pomocí elektronické správy účtů, pokud se banka s klientem nedohodnou jinak. Po dobu tří měsíců ode dne zrušení podúčtu může klient nadále získávat všechny informace o něm, včetně pohybů na účtu či podúčtu.

Čl. V. Žádosti o vydání platebních karet

1. Prostřednictvím internetbankingu lze bance zaslat žádost o vydání platební karty. Banka platební kartu klientovi vydá na základě uzavřené Žádosti/smlouvy o vydání platební karty prostřednictvím elektronických prostředků, je-li to výslovně uvedeno jako jedna z možností čl. VIII.

Čl. VI. Rozsah odpovědnosti stran

1. Klient odpovídá za závazky vzniklé elektronickým podáním pokynu stejně, jako by byl pokyn nebo žádost podán písemně.
2. Klient odpovídá za logickou správnost a soulad veškerých svých elektronicky podaných pokynů se smlouvou a Podmínkami, případně dalšími předpisy.
3. Klient odpovídá za škodu, pokud škodu způsobil svým podvodným jednáním, úmyslně nebo z hrubé nedbalosti. Hrubou nedbalostí se rozumí porušení jakékoli povinnosti klienta vyplývající z článku II, III,IX, X, XII až XIV, XV, XVa, XVI a XVIa Podmínek, zejména porušení opatření za účelem zajištění bezpečnosti a utajení důvěrných údajů, porušení povinností k zabezpečení počítače používaného pro přístup do internetbankingu, porušení povinností k zabezpečení mobilního zařízení/SIM karty používané pro zasílání SMS kódů, porušení povinnosti ověřit identifikaci serveru banky nebo aplikace pro elektronický podpis nebo porušení povinnosti včas oznámit bance podezření na zneužití bezpečnostních údajů.
4. Banka odpovídá za bezchybnost zpracování požadavků klienta, které jsou jí předány v souladu se smlouvou a Podmínkami. Banka nenese žádnou odpovědnost za případné škody vzniklé z důvodu poruchy přenosové sítě či z důvodu náhody, tj. nepředvídatelné a na vůli banky nezávislé události, jejíž následky nemohla banka odvrátit.
5. Banka odpovídá za nesprávné provedení pokynu, ledaže klientovi doloží, že částka nesprávně provedeného pokynu byla řádně a včas připsána na účet poskytovatele příjemce.
6. Banka neodpovídá za neautorizovaný nebo nesprávně provedený pokyn, jestliže ho klient neoznámil bance bez zbytečného odkladu, nejpozději však do 13 měsíců ode dne odepsání peněžních prostředků z příslušného účtu.

Čl. VII. Smluvní odměna a poplatky

1. Výše odměny účtovaná bankou za umožnění elektronické správy účtů je uvedena v Ceníku finančních operací a služeb, který vydává banka. Ceník může být vydán ve formě několika dílčích ceníků. Náklady na komunikaci s bankou hradí klient.
2. Poplatky za provedené pokyny pomocí elektronické správy účtů a poplatky za využití informačních a autorizačních prostředků jsou rovněž uvedeny v Ceníku finančních operací a služeb.

Čl. VIII. Pokyny a informace, které lze podávat, resp. získávat prostřednictvím el. správy účtů

1. Prostřednictvím elektronické aplikace internetbanking, jež slouží jako komunikační program mezi bankou a klientem, je klient zejména oprávněn zadávat pokyny bance, přijímat od banky informace, zprávy, upozornění, nabídky na platební či bankovní služby, uzavírat s bankou konkrétní smlouvy a i jinak komunikovat s bankou. Z toho důvodu je klient povinen

sledovat veškeré zprávy, informace a upozornění, které mu banka prostřednictvím internetbankingu doručí. Neplnění této povinnosti je porušení povinností vyplývajících ze smlouvy.

2. Klient souhlasí s tím, že banka v případech, kde to právní předpisy nevylučují, bude používat naskenovaný podpis jako mechanický prostředek náhrady vlastnoručního podpisu ve smluvních vztazích s klientem založených touto smlouvou a upravených těmito Podmínkami . Klient bere na vědomí, že takovou praxi banka považuje za obvyklou.
3. Banka i klient souhlasí, že v rámci kontaktu klienta s bankou prostřednictvím internetbankingu bude autorizace pokynů klienta v internetbankingu považována jako mechanický prostředek náhrady jeho vlastnoručního podpisu, kde to právní předpisy nevylučují. Klient prohlašuje, že takovou praxi bere za obvyklou.
4. Klient souhlasí, že banka má právo používat internetbanking, e-mailové zprávy, kurýra, službu krátkých textových zpráv (SMS) nebo jiných prostředků dálkové komunikace umožňující komunikaci s klientem s cílem nabídnout mu jakékoliv služby spojené se zřízením platebních a bankovních služeb. Klient souhlasí s poskytnutím jakýchkoliv informací, materiálů a nabídek způsobem uvedeným v předchozí větě tohoto odstavce.
5. V případech, kdy banka bude klientovi doručovat jakýkoliv dokument prostřednictvím internetbankingu, bude se považovat dokument za doručený v okamžiku, kdy banka obdrží potvrzení o jeho přečtení ze strany klienta, nejpozději však dnem následujícím po odeslání dokumentu, pokud klient neprokáže, že se z důvodů nezávislých na jeho vůli nemohl s obsahem zaslaného dokumentu seznámit.
6. V případech doručování kurýrem se považuje za den doručení den přijetí zásilky klientem.
7. Elektronickou správou účtů lze, není-li dále uvedeno jinak, zejména podávat tyto pokyny:
   - podání/ změna/rušení řádné výpovědi na vklad s výpovědní lhůtou nebo spořící účet s výpovědní lhůtou,
   - příkaz k úhradě finančních prostředků,
   - odvolání příkazu k úhradě finančních prostředků, jehož splatnost teprve nastane,
   - trvalý příkaz k úhradě finančních prostředků z běžného účtu nebo běžného vkladu,
   - změna/rušení trvalého příkazu k úhradě z běžného účtu nebo běžného vkladu,
   - zřízení/změna/zrušení souhlasu s inkasem ve prospěch jiného účtu
   - zřízení/změna/zrušení souhlasu s platbami SIPO,
   - avizování výběru hotovosti pobočce banky,
   - zřizování podúčtů a rušení podúčtů, rušení účtů[1] s výjimkou účtů dle čl. IV., odst.2. Podmínek,
   - změna způsobu připisování úroků, dispozice s úroky a dispozice se zůstatkem účtu nebo podúčtu po jeho zrušení,
   - změna hesla (pro internetbanking či smartbanking),
   - zmocnění třetí osoby ke správě účtu majitele,
   - zřízení/zrušení informačního hlásiče o událostech na účtu,
   - zřízení/zrušení smartbankingu a zadání přístupového hesla pro smartbanking a UID mobilního zařízení pro smartbanking,
   - zřízení/změna/zrušení PINu pro smartbanking,
   - změna UID mobilního zařízení pro smartbanking,
   - změna šifrovacího klíče;
   - změna způsobu a frekvenci předávání výpisů z účtů;
   - uzavření Smlouvy o vydání platební karty;
   - volba/změna vlastního PINu platební karty;
   - změna výše limitu pro platební karty;
   - změna stavu platební karty.
8. Elektronickou správou účtů lze zejména získávat tyto informace:
   parametry účtu a podúčtu, zůstatek na účtu nebo podúčtu k určitému datu, pohyby na účtu nebo podúčtu za určité období, výpis z účtu nebo podúčtu, přehled podaných pokynů spolu s jejich stavy, parametry vydané platební karty apod.
9. Pokyny dle odst. 7 musí být autorizovány dle čl. III. odst. 1. Podmínek. Některé z pokynů a informací, které lze podávat, resp. získávat prostřednictvím el. správy účtů, uváděné v odst. 7 a 8, mohou být při použití smartbankingu omezeny v závislosti na verzi aplikace, mobilního zařízení či jeho operačního systému.
10. Elektronickou správou účtů lze zadat požadavek na založení nebo zrušení informačního hlásiče o některých událostech na účtu. Klient si může zvolit hlásič dle aktuální nabídky přístupné klientovi v rámci elektronické správy účtu. Klient je oprávněn zvolit možnost zasílání informací o událostech na účtu formou sms nebo e-mailu na jím zadaný kontakt.

Čl. IX. Bezpečnostní upozornění související s využíváním internetbankingu

1. V souvislosti s poskytováním služeb elektronických komunikací, si Vás dovolujeme informovat o některých bezpečnostních rizicích s tím spojených a upozornit Vás na základní možnosti, kterými můžete Vy, jako uživatel, ochránit svoje osobní údaje, přihlašovací jméno a přístupové heslo do internetbankingu, elektronický klíč, heslo chránící elektronický klíč, PIN pro smartbanking, případně zaslaný sms kód, telefonní číslo, UID mobilního zařízení a jiné důvěrné nebo citlivé údaje (dále také „důvěrné informace“) a počítač před jejich zneužitím. Jde o základní pravidla, která je třeba dodržovat k ochraně Vašich důvěrných údajů a Vašeho počítače.
2. Banka a klient berou na vědomí, že zajištění bezpečnosti důvěrných informací při poskytování služeb elektronických komunikací je odpovědností obou smluvních stran v rozsahu jejich sféry vlivu, a že zavedení a dodržování některých preventivních opatření může vyžadovat finanční náklady.
3. Banka je povinna na své náklady provést ve své sféře vlivu taková technická a organizační opatření za účelem zajištění bezpečnosti důvěrných údajů, která jsou s ohledem na obvyklá rizika porušení ochrany důvěrných údajů technicky možná a přiměřená.
4. Klient je povinen na své náklady provést ve své sféře vlivu taková opatření za účelem zajištění bezpečnosti důvěrných údajů, která jsou s ohledem na obvyklá rizika porušení ochrany důvěrných údajů technicky možná a přiměřená. Klient bere na vědomí rizika spojená s poskytováním služeb elektronických komunikací a zavazuje se dodržovat zejména níže uvedená preventivní opatření a postupy k zajištění bezpečnosti důvěrných údajů. Nedodržení těchto pravidel a opatření může vést k zneužití důvěrných údajů a ke vzniku škody klientovi nebo třetí osobě.
5. S ohledem na co nejvyšší ochranu důvěrných údajů a majetku klienta doporučuje banka, aby si klient sjednal s bankou autorizaci elektronických pokynů pomocí sms zpráv nebo autorizaci prostřednictvím elektronického podpisu a využíval pro zadávání svého hesla při přihlašování do internetbankingu grafickou klávesnici.

Čl. X. Rizika plynoucí z poskytování služeb elektronických komunikací

1. Služby elektronických komunikací jsou poskytovány prostřednictvím datových případně telefonních linek (dále také „datové linky“), které neprovozuje banka, ale třetí osoba odlišná od banky. Zabezpečení těchto datových linek je mimo sféru vlivu banky a banka není proto schopna zcela zabránit všem možným rizikům zneužití důvěrných údajů v průběhu přenosu prostřednictvím datové linky. Při přenosu důvěrných údajů nelze proto zcela vyloučit riziko neoprávněného získání důvěrných informací třetí osobou (např. hrozba tzv. hackerů,

[1] Rušit účty, případně jinak nakládat s účty, smí pouze majitel účtu a osoba k tomu majitelem účtu zmocněná.

interní rizika provozovatele datové sítě, tzv. Man in the middle, tj. odposlouchávání komunikace třetí osobou předstírající protistranu komunikace, odposlouchávání telefonických hovorů, podvržení dat apod.).

2. Některá rizika plynoucí z poskytování služeb elektronických komunikací mohou být také ve sféře vlivu klienta. Mezi tato rizika patří zejména nedostatečné zabezpečení počítače klienta, který je používán pro přihlášení do internebankingu a k podávání pokynů bance a dále nesprávné nakládání s důvěrnými údaji klientem a z toho plynoucí možnost jejich zneužití ze strany třetích osob.
3. Banka neodpovídá za případnou škodu klienta nebo třetích osob vzniklou zneužitím důvěrných informací neoprávněně získaných z datových linek mimo sféru vlivu banky, počítače klienta nebo v důsledku nesprávného nakládání s těmito údaji klientem, pokud nejde o případ porušení povinnosti na straně banky.

Čl. XI. Preventivní opatření prováděná bankou

1. Banka provádí ve své sféře vlivu preventivní opatření snižující riziko zneužití důvěrných informací. Mezi tato opatření patří zejména šifrování veškerých dat (tj. např. uživatelské jméno a heslo do internetbankingu), která jsou přenášena mezi počítačem klienta a serverem Fio. Veškerá data jsou šifrována standardem SSL 128bit. Šifrování přenášených dat výrazně snižuje možnost zjištění důvěrných údajů o klientovi třetí osobou při přenosu datovou linkou a jejich následné zneužití.
2. Banka dále umožňuje klientovi využívat další bezpečnostní prvky chránící přístup do internetbankingu, mezi které patří možnost využití grafické klávesnice pro zadávání hesla při přihlašování do internetbankingu, což snižuje riziko neoprávněného zjištění těchto údajů třetí osobou a možnost potvrzování pokynů elektronickým způsobem podávaných klientem podle komisionářské smlouvy formou sms zpráv na individuálně stanovené telefonní číslo klienta nebo formou elektronického podpisu.
3. Informace o některých bezpečnostních opatřeních souvisejících s obchodováním klienta jsou uvedeny také na této webové adrese: http://www.fio.cz/bankovni-sluzby/internetbanking.

Čl. XII. Utajení důvěrných údajů

1. Chraňte své důvěrné údaje před zveřejněním a zneužitím.
2. Důvěrné údaje si nezaznamenávejte. Pokud si důvěrné údaje přesto poznamenáte, uschovejte je na místě, které není volně přístupné dalším osobám.
3. Neuvádějte důvěrné údaje tak, aby se dala spojit s příslušným účtem (např. napsání důvěrných údajů v dokladech spojených s účtem, automatické zapamatování přihlašovacího jména a hesla do internetbankingu počítačem).
4. Nezadávejte důvěrné údaje před jinou osobou, nesdělujte důvěrné údaje jiným osobám, a to ani rodinným příslušníkům a osobám blízkým.
5. Vaše heslo stanovte nejlépe jako kombinaci čísel a velkých a malých písmen, bez osobního vztahu k Vám nebo osobám blízkým. Jednoduché heslo s osobními rysy je snáze odhalitelné. Jako heslo a PIN pro smartbanking nepoužívejte svoje datum narození, rodné číslo, telefonní číslo, po sobě jdoucí číslice apod. Heslo a PIN pro smartbanking pravidelně měňte. Nikdy neměňte heslo do internetbankingu na jiném formuláři, než v záložce Globální nastavení v internetbankingu. Banka po Vás v žádném případě nebude vyžadovat jiný postup. Prvotní heslo musíte změnit při prvním přihlášení do internetbankingu. Platnost následujícího hesla je z bezpečnostních důvodů omezena na 365 dnů. Vyprší-li tato lhůta, budete při nejbližším přihlášení do internetbankingu vyzváni k jeho změně.
6. Nezasílejte důvěrné údaje pomocí e-mailu nebo sms, nezadávejte je na jiné internetové stránce, než na stránce určené k přihlášení do internetbankingu, a to ani v případě že obdržíte e-mail případně sms, která napodobuje výzvu, zejména od banky, k zaslání důvěrných údajů nebo jejich vyplnění na jiné internetové stránce. Banka Vám takový druh zpráv v žádném případě nebude zasílat.

Čl. XIII. Uložení elektronického klíče

1. Chraňte svůj elektronický klíč, který používáte při zadávání pokynů, proti jeho zneužití, zejména proti jeho odcizení, okopírování apod. Zneužitím Vašeho elektronického klíče může jiná osoba předstírat Vaši identitu a zadávat pokyny Vaším jménem. Zneužití elektronického klíče Vám může způsobit škodu.
2. Elektronický klíč instalujte pouze na počítač, o kterém víte, že je chráněn proti možným hrozbám plynoucím z připojení k datové síti. Neinstalujte a nepoužívejte elektronický klíč na počítač, který je veřejně přístupný.
3. Uchováváte-li elektronický klíč na jiném přenosném médiu, ukládejte toto médium na místo, kde nedojde k jeho zneužití, zejména odcizení, okopírování nebo poškození.

Čl. XIV. Preventivní opatření ve sféře vlivu klienta, zabezpečení počítače klienta

1. Internetbanking používejte pouze na počítačích, které jsou řádně zabezpečené proti zneužití důvěrných údajů. Nepoužívejte internetbanking zejména v internetových kavárnách a na jiných veřejně přístupných počítačích, ani na počítačích, u kterých nemáte jistotu, že jsou zabezpečeny proti zneužití důvěrných údajů.
2. Před přihlášením do internetbankingu se řádně přesvědčte, že komunikujete se správným poskytovatelem služby. Adresa serveru banky je http://www.fio.cz/. Při přihlašování do aplikace internetbanking a při zadávání pokynů prostřednictvím aplikace internetbanking řádně zkontrolujte, že spojení je zabezpečeno (ověřte platnost certifikátu SSL zabezpečení) a dále ověřte identifikaci serveru banky. V případě pochybností o tom, že komunikujete s bankou nebo, že spojení není řádně zabezpečeno, neprovádějte žádné úkony, které by mohly vést k prozrazení nebo zneužití důvěrných údajů a bezodkladně kontaktujte klientského pracovníka banky.
3. Počítač, na kterém se rozhodnete používat internetbanking, zabezpečte legálním firewallem, antivirovou a anti-spyware ochranou, a tyto ochranné prvky pravidelně aktualizujte. Programy aktualizujte standardním způsobem. Pravidelně sledujte informace o nových hrozbách, virech, spyware apod. a v souladu s tím zajistěte ochranu Vašeho počítače.
4. Používejte legální a pravidelně aktualizovaný operační systém ve Vašem počítači. Pravidelně sledujte zprávy výrobce Vašeho operačního systému o opravách chyb a nedostatků tohoto operačního systému a tyto opravy včas instalujte do Vašeho počítače.
5. Používáte-li internetbanking na určitém počítači, vyvarujte se stahování a instalování programů, které lze volně získat na internetu, u nichž si nejste jisti, zda neobsahují viry nebo spyware, případně nepocházejí ze zdroje, který je důvěryhodný. Navštěvujte pouze známé, důvěryhodné a bezpečné stránky na internetu. Neotvírejte nevyžádané emaily, emaily od neznámých adresátů a emaily s podezřelým názvem nebo obsahem na takovém počítači. Takové emaily bez otevření smažte. Ve své emailové schránce používejte spam filter.
6. Žádná licenční ujednání u volně šířeného softwaru Vám nemohou poskytnout jistotu, že software neobsahuje součásti, které mohou Váš počítač poškodit či jinak narušit bezpečnost Vámi ukládaných údajů.
7. Pro získání základních informací o možnostech zabezpečení Vašeho počítače a o rizicích, která hrozí Vašemu počítači si prosím přečtěte informace na stránkách: www.microsoft.com/cze/athome/security/protect/

Čl. XV. Zabezpečení sms a mobilního zařízení

1. Pro přijímání autorizačních sms kódů je nejdůležitější SIM karta, která obsahuje telefonní číslo, které jste určili k přijímání autorizačních sms kódů od banky (dále jen „SIM karta“). Tuto SIM kartu mějte vždy pod dohledem, mobilní zařízení bez SIM karty neumožní komunikaci s bankou a autorizaci.
2. Mobilní zařízení či SIM kartu, neponechávejte ležet na místech, kde nad nimi nemáte dohled.
3. Vyvarujte se půjčování mobilního zařízení či SIM karty, třetím osobám, aniž byste měli přehled o jejich nakládání s mobilním zařízením a SIM kartou.
4. V případě, že hrozí riziko, že byste mohli ponechat mobilní zařízení mimo Váš dohled, znemožněte jeho používání třetím osobám kódem PIN. Tento kód uchovávejte v tajnosti a nesdělujte ho třetím osobám, ani si ho nikam nepoznamenávejte.
5. Autorizační kód doručený Vám bankou si nikam nepoznamenávejte a sms s autorizačním kódem žádné osobě nezpřístupňujte.
6. V závislosti na technickém pokroku v oblasti funkcí mobilních zařízení zajistěte funkce svého mobilního zařízení proti možnosti automatického připojení třetí osoby k Vašemu mobilnímu zařízení.
7. Pro smartbanking a zasílání autorizace PINem je nejdůležitější mobilní zařízení, jehož UID jste určili pro tento druh služby. Toto mobilní zařízení mějte vždy pod dohledem, pro jeho zabezpečení platí obdobně pravidla pro mobilní zařízení uvedená výše. Vždy se odhlaste z aplikace smartbanking bezprostředně po ukončení práce s ní a nikdy nepůjčujte ani neponechávejte mimo dohled své mobilní zařízení, jste-li přihlášeni do aplikace smartbanking.

Čl. XVa. Blokace internetbankingu a smartbankingu

1. Banka je oprávněna trvale nebo dočasně zablokovat internetbanking v případě, že:
   a) vznikne podezření ze zneužití internetbankingu nebo dojde ke zneužití internetbankingu,
   b) se významně zvýší riziko, že klient nebude schopen splácet úvěr, který lze čerpat prostřednictvím internetbankingu.
2. Banka je oprávněna trvale nebo dočasně zablokovat smartbanking v případě, že vznikne podezření ze zneužití smartbankingu nebo dojde ke zneužití smartbankingu.

Čl. XVI. Kontaktujte klientského pracovníka

1. V případě, že obdržíte e-mail s upozorněním na jakoukoli změnu ve způsobu přihlašování do internetbankingu nebo s informací o změně www adresy přihlašovací stránky, nebo v případě, že zjistíte netypické nebo jinak podezřelé chování přihlašovací stránky, včetně automatického přesměrování, nebo jiné podezřelé skutečnosti, neprovádějte žádné úkony, které by mohly vést k prozrazení nebo zneužití důvěrných údajů a bezodkladně kontaktujte telefonicky klientské pracovníky banky a vyžádejte si radu ohledně dalšího postupu.

Čl. XVIa. Oznámení o zneužití internetbankingu

1. Klient je povinen bance neprodleně oznámit ztrátu, odcizení nebo zneužití přihlašovacího jména a hesla do internetbankingu či smartbankingu, elektronického podpisu, mobilního zařízení (SIM karty), na které se zasílají sms kódy, mobilního zařízení s aplikací smartbanking, nebo jiných důvěrných informací.
2. Klient oznámí ztrátu, odcizení nebo zneužití výše uvedených údajů telefonicky na tel. číslo: 224 346 797. Tato telefonní linka je klientovi k dispozici nepřetržitě kterýkoliv den v roce. Při oznámení je klient povinen uvést alespoň tyto údaje: osobní identifikační údaje a svoje přihlašovací jméno do internetbankingu. Bez sdělení těchto údajů se nepovažuje oznámení klienta za řádné a banka není povinna takové oznámení přijmout. V případě řádného oznámení je banka oprávněna, ale nikoli povinna ověřit toto oznámení např. zpětným kontaktováním klienta. Klient souhlasí s tím, že banka je oprávněna z preventivních a bezpečnostních důvodů od okamžiku řádného přijetí oznámení dle tohoto článku neprovést žádné již podané nebo již přijaté pokyny na vrub účtu, ke kterému má klient přístup na základě sděleného přihlašovacího jména do internetbankingu a zablokovat přístup do internetbankingu na základě tohoto uživatelského jména. Banka není odpovědná za škodu způsobenou klientovi z důvodu provedení bezpečnostních opatření podle tohoto dle tohoto článku.

Čl. XVII. Závěrečná ustanovení

1. V zájmu zlepšení kvality služeb poskytovaných klientovi, v souvislosti se změnou identifikace (fingerprintu) serveru banky, v návaznosti na vývoj právního prostředí a také s ohledem na obchodní politiku banky je banka oprávněna tyto Podmínky měnit a doplňovat (vyhlašovat nové znění). Banka je oprávněna navrhnout klientovi změnu smlouvy o elektronické správě účtu a těchto obchodních podmínek (dále také „návrh na změnu smlouvy“). Návrh na změnu smlouvy se klientovi poskytuje alespoň 2 měsíce před předpokládanou účinností změny, a to prostřednictvím internetbankingu. Návrh na změnu smlouvy se stává pro klienta závazný, jestliže byl návrh poskytnut klientovi způsobem a ve lhůtě podle předchozí věty, klient návrh na změnu smlouvy neodmítl, ačkoli byl o tom v souvislosti s návrhem na změnu smlouvy poučen a smlouvu o elektronické správě účtu, nevypověděl, ačkoli byl o tom v souvislosti s návrhem na změnu smlouvy poučen. Klient je oprávněn návrh na změnu smlouvy odmítnout a smlouvu vypovědět, jestliže mu nebyla změna poskytnuta alespoň 2 měsíce před předpokládanou účinností změny. Jestliže klient odmítne návrh na změnu smlouvy, považuje se to automaticky za výpověď smlouvy o elektronické správě účtu podanou bankou, pokud nestanoví banka jinak. Odmítnutí návrhu na změnu smlouvy a výpověď smlouvy klientem musí být v písemné podobě. Takto vypovězená smlouva zanikne ke dni účinnosti navrhované změny. Klient je kdykoli oprávněn po dobu výpovědní lhůty odvolat svůj nesouhlas s návrhem změny. Odmítnutí návrhu na změnu a případné odvolání tohoto nesouhlasu bance se doručuje bance na adresu jejího sídla nebo příslušné pobočky. Návrh na změnu smlouvy se stává pro klienta závazný uplynutím stanovené lhůty, jestliže byl návrh poskytnut klientovi výše uvedeným způsobem. Klient žádá banku, aby mu byl návrh na změnu smlouvy nebo obchodních podmínek zaslán prostřednictvím internetbankingu do této aplikace v podobě nového úplného znění smlouvy tak, aby mohl tento návrh uchovat a využívat po přiměřenou dobu a mohl tento návrh v nezměněné podobě reprodukovat. Banka žádost klienta přijímá.
2. Ve vztahu ke Smlouvám o elektronické správě účtů nebo Smlouvám o vydání platební karty uzavřeným od 18.6.2012, pokud k nim byly tyto Podmínky přiloženy, jsou tyto Podmínky platné a účinné uzavřením smlouvy nebo Smlouvy o vydání platebních karet. Ve vztahu k ostatním Smlouvám o elektronické správě účtů jsou tyto Podmínky účinné dnem 21.8.2012. Nabytím účinnosti těchto Podmínek podle druhé věty tohoto odstavce pozbývají platnosti „Obchodní podmínky pro elektronickou správu účtů vedených bankou Fio banka, a.s.“ ze dne 26.5.2011 (účinné od 27.7.2011).

V Praze dne 18.6.2012

Mgr. Jan Sochor, v.r.	Mgr. Josef Valter, v.r.
předseda představenstva	člen představenstva
Fio banka, a.s.	Fio banka, a..s