Obchodní podmínky pro elektronickou správu účtů

vedených bankou Fio banka, a.s., IČ: 61858374, Praha 1, V Celnici 1028/10, PSČ: 117 21, zapsanou v obchodním rejstříku vedeném rejstříkovým soudem v Praze, oddíl 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 níž 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 (smartphone) či tabletem (dále též jen souhrnné označení „zařízení“ pro počítač, mobilní telefon, tablet a obdobné mobilní zařízení) klienta prostřednictvím internetu. Adresa serveru banky je www.fio.cz; další adresy banky jsou: www.fio.sk, www1.fio.cz, www2.fio.cz, www3.fio.cz, www.fiobanka.com, www.fio.hu, www.e-broker.cz, ib.fio.cz, ib.fio.sk. Banka má právo kdykoliv omezit přístup na kterýkoliv ze serverů banky, a to dočasně i trvale. Přenášená data jsou zabezpečena prostřednictvím šifrované komunikace (https) za pomoci certifikátu SSL serveru od společnosti GeoTrust Inc.
2. Klient je před každým využitím služeb banky poskytovaných prostřednictvím internetu (zejména služeb Internetbanking a e-Broker) a před každým zadáním důvěrných údajů do přihlašovacího dialogu povinen nejprve ověřit, zda jsou z jeho strany dodrženy všechny povinnosti uložené ve smyslu článku XIV "Bezpečnostní opatření ve sféře klienta, zabezpečení zařízení klienta", odst. 1. Banka neodpovídá za škodu způsobenou porušením této povinnosti. Další povinnosti klienta související s omezením rizik při používání služeb banky prostřednictvím internetu, jako i důležité informace a upozornění na rizika týkající se využívání služeb banky prostřednictvím internetu, jsou uvedeny v čl. IX až XVIa Podmínek.
3. 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. Aplikace smartbanking může na některých mobilních zařízeních umožnit nahrazení PINu pro smartbanking nebo přístupových údajů pro smartbanking (vždy ale maximálně jednoho z těchto bezpečnostních prvků) použitím zabudovaného biometrického snímače. 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. VIII odst. 9 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 vygenerovaným 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.

3b. Autorizace za použití biometrického snímače. Pokud je již nastaven způsob autorizace podle odst. 3a, na vybraných mobilních zařízeních může aplikace smartbanking umožnit nahrazení PINu pro smartbanking nebo přístupových údajů pro smartbanking (vždy ale maximálně jednoho z těchto bezpečnostních prvků) použitím zabudovaného biometrického snímače. Možnost použití biometrického snímače klient nastaví v aplikaci smartbanking a jeho nastavení autorizuje PINem pro smartbanking. Před nastavením použití biometrického snímače banka doporučuje klientovi seznámit se s principy jeho fungování v použitém mobilním zařízení. Banka neodpovídá za správné fungování biometrického snímače a klient nastavením jeho použití pro smartbanking na sebe přebírá riziko vyplývající z možných chyb jeho fungování. Aplikace smartbanking ani jiné systémy banky nezískávají, nezpracovávají ani neukládají žádná biometrická data klienta. Zrušení možnosti použití biometrického snímače se nastavuje potvrzením příslušné volby v smartbankingu. Pro alternativní autorizaci pomocí passcode do telefonu platí stejná pravidla a povinnosti jako pro autorizaci za pomocí biometrického snímače.

4. Nastavení způsobu a podmínek autorizace dle odst. 2 a odst. 3 konkrétního klienta je uvedeno v Protokolu o nastavení autorizace elektronických pokynů. Nastavení způsobu a podmínek autorizace PINem pro smartbanking dle odst. 3a a případně následné nastavení autorizace za použití biometrického snímače podle odst. 3b je považováno za nastavenou autorizaci elektronických pokynů podle Smlouvy o elektronické správě účtů okamžikem zřízení smartbankingu klientem prostřednictvím internetového rozhraní internetbankingu (resp. okamžikem nastavení použití biometrického snímače podle odst. 3b), 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. Způsob a podmínky autorizace dle odst. 3b může klient změnit elektronicky prostřednictvím aplikace smartbanking.

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, XVI a XVIa Podmínek, zejména porušení opatření za účelem zajištění bezpečnosti a utajení důvěrných údajů, porušení povinností k zabezpečení zařízení 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;
   - volba použití biometrického snímače v mobilním zařízení pro smartbanking (toto lze nastavit pouze přes smartbanking).
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. Některé pokyny dle odst. 7, dle požadavků banky týkajících se autorizace a aktuálních v čase zadávání pokynu, musí být autorizovány dle čl. III. 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.
11. Příkazem k úhradě se pro účely Podmínek rozumí i příkaz k tzv. dobití kreditu (banka může označit i jiným obdobným názvem srozumitelným pro běžného klienta), tj. příkaz k úhradě finančních prostředků ve prospěch účtu příslušného mobilního operátora za účelem dobití kreditu SIM karty (tj. za účelem předplacení služeb poskytovaných mobilním operátorem jeho zákazníkovi) identifikované klientem při zadávání pokynu uvedením telefonního čísla příslušné SIM karty; klient u zadání pokynu nezadává číslo účtu mobilního operátora (příjemce převodu), ale zadá telefonní číslo příslušné SIM

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

karty, jejíž kredit má být převodem dobit, případně určí i příslušného mobilního operátora (je-li to vyžadováno) a zadá jiné bankou požadované údaje.

Čl. IX. Bezpečnostní upozornění související s využíváním internetbankingu

1. V souvislosti s poskytováním služeb elektronických komunikací, banka si dovoluje informovat klienta o některých bezpečnostních rizicích s tím spojených a upozornit klienta na základní možnosti, kterými může, 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, kód (passcode, PIN) pro přístup k mobilnímu zařízení a jiné důvěrné nebo citlivé údaje (dále také „důvěrné informace“) a zařízení před jejich zneužitím. Jde o základní pravidla, která je třeba dodržovat k ochraně důvěrných údajů a zařízení klienta.
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 a bezpečností 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, 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 zařízení 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, zařízení 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 zařízením 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. Klient má povinnost chránit své důvěrné údaje před zveřejněním a zneužitím.
2. Klient má povinnost nezaznamenávat si důvěrné údaje. Pokud si důvěrné údaje klient přesto poznamená, klient je povinen uschovat důvěrné údaje jednotlivě od ostatních důvěrných údajů a na místě, které není volně přístupné dalším osobám.
3. Klient má povinnost neuvádět 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 zařízením).
4. Klient má povinnost dodržovat dostatečnou míru obezřetnosti při správě důvěrných údajů, zejména nezadávat důvěrné údaje před jinou osobou, nesdělovat důvěrné údaje jiným osobám, a to ani rodinným příslušníkům a osobám blízkým. Za porušení těchto podmínek se však nepovažuje sdělení uživatelského jména jiné fyzické osobě za účelem zřízení oprávnění k účtu této osoby, resp. k účtu touto osobou ovládanému.
5. Klient má povinnost stanovit heslo jako kombinaci čísel a velkých a malých písmen, bez osobního vztahu ke své osobě nebo osobám blízkým. Jednoduché heslo s osobními rysy je snáze odhalitelné. Klient nesmí použít jako heslo a PIN pro smartbanking svoje datum narození, rodné číslo, telefonní číslo, po sobě jdoucí číslice apod. Klient má povinnost heslo a PIN pro smartbanking pravidelně měnit. Klient nesmí měnit heslo do internetbankingu na jiném formuláři, než v záložce Globální nastavení v internetbankingu. Banka nebude v žádném případě vyžadovat po klientovi jiný postup. Prvotní heslo musí klient změnit při prvním přihlášení do internetbankingu. Platnost následujícího hesla je z bezpečnostních důvodů omezena na 365 dnů. Vyprší-li tato lhůta, bude klient při nejbližším přihlášení do internetbankingu vyzván k jeho změně.
6. Klient má povinnost dodržovat dostatečnou míru obezřetnosti při zadávání důvěrných údajů, zejména nezasílat důvěrné údaje pomocí e-mailu nebo sms, nezadávat je na jiné internetové stránce, než na stránce určené k přihlášení do

internetbankingu, a to ani v případě, že klient obdrží e-mail případně sms, která napodobuje výzvu, zejména od banky, k zaslání důvěrných údajů nebo jejich vyplnění na jiné internetové stránce. Banka nebude v žádném případě zasílat takový druh zpráv klientovi.

Čl. XIII. Uložení elektronického klíče

1. Klient má povinnost chránit svůj elektronický klíč, který používá při zadávání pokynů, proti jeho zneužití, zejména proti jeho odcizení, okopírování apod. Zneužitím elektronického klíče klienta může jiná osoba předstírat identitu klienta a zadávat pokyny jménem klienta. Zneužití elektronického klíče může způsobit klientovi škodu.
2. Klient má povinnost elektronický klíč instalovat pouze na počítač, na kterém si může být s dostatečnou mírou jist, že je chráněn proti možným hrozbám plynoucím z připojení k datové síti. Klient nesmí instalovat a používat elektronický klíč na počítači, který je veřejně přístupný.
3. Pokud klient uchovává elektronický klíč na jiném přenosném médiu, tak má klient povinnost ukládat toto médium na místo, kde je do velké míry omezeno riziko jeho zneužití, zejména odcizení, okopírování nebo poškození.

Čl. XIV. Bezpečnostní opatření ve sféře vlivu klienta, zabezpečení zařízení klienta

1. Klient má povinnost se řídit všemi povinnostmi, které jsou mu uloženy v odstavcích 2 až 12 tohoto článku. Všechny informace zahrnuty v odstavcích 2 až 12 tohoto článku jsou povinnosti.
2. Klient má povinnost internetbanking používat pouze na zařízeních, která jsou řádně zabezpečená proti zneužití důvěrných údajů. Klient nesmí používat internetbanking zejména v internetových kavárnách a na jiných veřejně přístupných zařízeních, ani na zařízeních, u kterých nemá dostatečnou míru jistoty, že jsou zabezpečeny proti zneužití důvěrných údajů. Klient je povinen využívat k internetbankingu jen takové zařízení, na kterém si může být s dostatečnou mírou jist práv, které má nastaven jako uživatel takového zařízení, stejně jako práv, které mají třetí osoby k tomuto zařízení, včetně práv umožňující dálkový přístup.
3. Klient má povinnost se před přihlášením do internetbankingu řádně přesvědčit, že komunikuje se správným poskytovatelem služby. Klient má povinnost vždy ověřit, že vstupní stránka má v prohlížeči jednu z těchto adres: www.fio.cz, www.fio.sk, www1.fio.cz, www2.fio.cz, www3. fio.cz, www.fiobanka.com, www.fio.hu, www.e-broker.cz, ib.fio.cz, ib.fio.sk. Banka má právo kdykoliv omezit přístup na kteroukoli z uvedených adres, a to dočasně i trvale.
4. Klient má povinnost při přihlašování do aplikace internetbanking a při zadávání pokynů prostřednictvím aplikace internetbanking řádně zkontrolovat, že spojení je zabezpečeno (ověřit platnost certifikátu SSL zabezpečení) a dále ověřit identifikaci serveru banky. Při využívání služeb banky poskytovaných prostřednictvím internetu (zejména internetbanking a e-Broker) je klient vždy povinen si zkontrolovat, že komunikuje s bankou šifrovanou komunikací (https) za použití certifikátu SSL serveru a dále je v uvedených případech, při každém svém připojení na server banky, povinen ověřit, zda certifikát SSL serveru je certifikátem s rozšířeným ověřením identity vydaným pro Fio Banka, a.s. Praha 1 Česká republika, CZ, zda certifikát SSL serveru vydala společnost GeoTrust Inc., zda certifikát SSL serveru je platný (datum platnosti nevypršelo) a také je povinen ověřit identifikaci certifikátu SSL serveru (SHA1 Fingerprint) porovnáním se správnou identifikací, která je dostupná na: https://www.fio.cz/docs/cz/sec/fingerprint.pdf. 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. Banka neodpovídá za škodu způsobenou porušením povinností stanovených v tomto odstavci klientem.
5. Klient je při každém svém připojení aplikací Fio-podpis (dále také „elektronický klíč“) povinen ověřit její identifikaci (SHA1 Fingerprint) porovnáním se správnou identifikací, která je dostupná na: https://www.fio.cz/docs/cz/sec/fingerprint.pdf. 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.
6. Identifikace dle odst. 4 a 5 je pravidelně měněna. Z tohoto důvodu je klient povinen při každém svém připojení na server banky ověřit aktuálnost identifikace. Její správné a aktuální znění získá na https://www.fio.cz/docs/cz/sec/fingerprint.pdf nebo na kterékoliv pobočce banky. Banka neodpovídá za škodu způsobenou porušením této povinnosti klientem.
7. Klient má povinnost v případě jakékoli pochybnosti o tom, že komunikuje s bankou, nebo že spojení není řádně zabezpečeno, neprovádět žádné úkony, které by mohly vést k prozrazení nebo zneužití důvěrných údajů, zejména zadání přihlašovacích údajů a bezodkladně kontaktovat pracovníka banky za pomocí linky technické podpory na telefonním čísle +420 224 346 392.
8. Klient má povinnost legálně zabezpečit zařízení, na kterém se rozhodne používat internetbanking, firewallem, antivirovou a anti-spyware ochranou, a tyto ochranné prvky pravidelně aktualizovat. Klient má povinnost aktualizovat programy standardním způsobem a pravidelně sledovat informace o nových hrozbách, virech, spyware apod. a v souladu s tím zajistit ochranu takového zařízení.
9. Klient má povinnost používat internetbanking pouze na zařízeních, kde je legálně pořízený a pravidelně aktualizovaný operační systém. Klient má povinnost pravidelně sledovat zprávy výrobce operačního systému o opravách chyb a nedostatků tohoto operačního systému a tyto opravy včas instalovat na zařízení, na kterém je používán internetbanking.
10. Klient je povinen používat důvěryhodný internetový prohlížeč, který pravidelně aktualizuje. Také je povinen nastavit zabezpečení tohoto prohlížeče standardním způsobem a kontrolovat vždy před zadáním přihlašovacích údajů, zda prohlížeč nehlásí jakékoli varování, obzvláště varování ohledně důvěryhodnosti certifikátu SSL serveru.
11. Klient má povinnost na zařízeních, na kterých používá internetbanking, vyvarovat se stahování a instalování programů, které lze volně získat na internetu, u nichž si nemůže být s dostatečnou mírou jist, že neobsahují viry nebo spyware, případně že nepocházejí ze zdroje, který je nedůvěryhodný. Klient má povinnost na zařízení, na kterém využívá internetbanking, navštěvovat pouze známé, důvěryhodné a bezpečné stránky na internetu a neotvírat nevyžádané emaily, emaily od neznámých adresátů a emaily s podezřelým názvem nebo obsahem na takovém zařízení. Takové emaily má klient povinnost bez otevření smazat. Klient má povinnost ve své emailové schránce používat spam filtr. Banka upozorňuje klienta, že žádná licenční ujednání u volně šířeného softwaru nemohou klientovi poskytnout jistotu, že software neobsahuje součásti, které mohou zařízení klienta poškodit či jinak narušit bezpečnost ukládaných údajů klienta.
12. Vyspělejší mobilní zařízení (zejména tzv. smartphony a tablety) s operačním systémem iOS, Android, Windows Phone a jiným operačním systémem, je nutné chránit obdobně jako počítač, a to prostřednictvím legálního antivirového programu; je rovněž žádoucí neinstalovat aplikace z jiných než oficiálních zdrojů pro příslušný operační systém mobilního zařízení (např.

Apple App Store, Google Play, Window Phone Store, atd.), banka však upozorňuje, že klient nemůže spoléhat na kontrolu prováděnou provozovatelem operačního systému ve vztahu ke všem aplikacím Klient má povinnost legálně zabezpečit takové mobilní zařízení firewallem, antivirovou a anti-spyware ochranou a tyto ochranné prvky pravidelně aktualizovat. Klient má v návaznosti na to povinnost tyto programy standardním způsobem aktualizovat, pravidelně sledovat informace o nových hrozbách, virech, spyware apod. a v souladu s tím uzpůsobovat ochranu mobilního zařízení.

13. Klientovi se doporučuje, aby si před každým zadáním důvěryhodných údajů ověřil, že zařízení, ze kterého se hlásí, používá DNS překladače podporující DNSSEC, a prohlížeč si nastavil tak, aby sám prováděl DNSSEC ověřování.
14. Banka doporučuje klientovi průběžně se obeznamovat s aktuálními informacemi o možnostech zabezpečení zařízení a o aktuálních rizicích, která při používání zařízení hrozí, a v případě, kdy klientovy znalosti dané problematiky nejsou pro řádné zabezpečení zařízení dostatečné, nebo kdy má klient sám o jejich dostatečnosti pochybnosti, banka doporučuje klientovi obrátit se s požadavkem na zabezpečení zařízení a jeho případného komunikačního příslušenství na odborníka.

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“). Mobilní zařízení bez SIM karty neumožní komunikaci s bankou a autorizaci.
2. Klient má povinnost mít mobilní zařízení či SIM kartu pod dohledem a neponechávat je ležet na místech, kde nad nimi nemá dohled.
3. Klient má povinnost vyvarovat se půjčování mobilního zařízení či SIM karty, třetím osobám, aniž by měl přehled o jejich nakládání s mobilním zařízením a SIM kartou.
4. V případě, že hrozí riziko, že by klient mohl ponechat mobilní zařízení mimo svůj dohled, klient má povinnost znemožnit jeho používání třetím osobám kódem PIN a tento kód uchovávat v tajnosti a nesdělovat ho třetím osobám, ani ho nikam nepoznamenávat.
5. Autorizační kód doručený klientovi bankou si klient nesmí nikam poznamenat a sms s autorizačním kódem nesmí žádné osobě zpřístupnit.
6. Klient má povinnost v závislosti na technickém pokroku v oblasti funkcí mobilních zařízení zajistit funkce svého mobilního zařízení proti možnosti automatického připojení třetí osoby k mobilnímu zařízení.
7. Pro smartbanking a autorizaci za využití aplikace smartbanking je nejdůležitější mobilní zařízení, jehož UID klient určil pro tento druh služby. Klient má povinnost mít takové mobilní zařízení vždy pod dohledem. Pro jeho zabezpečení platí obdobně pravidla pro mobilní zařízení uvedená výše. Klient má povinnost se vždy odhlásit z aplikace smartbanking bezprostředně po ukončení práce s ní a nikdy nepůjčovat ani neponechávat mimo dohled své mobilní zařízení, pokud je klient přihlášen do aplikace smartbanking.
8. I v případě, že na mobilním zařízení klient nepoužívá internetbanking ani smartbanking, ale přesto je v takovém mobilním zařízení zapojená SIM karta (tzn. SIM karta, která platí pro telefonní číslo, které je určeno k přijímání autorizačních sms kódů od banky), klient má povinnost legálně zabezpečit takové mobilní zařízení firewallem, antivirovou a anti-spyware ochranou a tyto ochranné prvky pravidelně aktualizovat. Klient má povinnost aktualizovat programy standardním způsobem a pravidelně sledovat informace o nových hrozbách, virech, spyware apod. a v souladu s tím zajistit ochranu takového zařízení. Postup uvedený v tomto odstavci slouží k omezení rizika utajeného přeposílání autorizačních sms kódů zasílaných bankou (v případě napadeného mobilního zařízení); alternativou k omezení uvedeného rizika je používání SIM karty výlučně v tzv. „hloupých“ telefonech.

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.
3. Banka je oprávněná trvale nebo dočasně zablokovat použití biometrického snímače pro aplikaci smartbanking v mobilním zařízení v případě, že vznikne podezření ze zneužití nebo dojde ke zneužití tohoto způsobu autorizace.

Čl. XVI. Kontaktujte klientského pracovníka

1. V případě, že klient obdrží 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 klient zjistí netypické nebo jinak podezřelé chování přihlašovací stránky, včetně automatického přesměrování, nebo jiné podezřelé skutečnosti, klient nesmí provádět žádné úkony, které by mohly vést k prozrazení nebo zneužití důvěrných údajů a je povinen bezodkladně kontaktovat pracovníka banky za pomocí linky technické podpory na telefonním čísle +420 224 346 392.

Čl. XVIa. Oznámení o zneužití internetbankingu a smartbankingu

1. Klient je povinen bance neprodleně oznámit ztrátu, odcizení nebo zneužití přihlašovacího jména a hesla do internetbankingu či smartbankingu, neautorizovaný přístup do smartbankingu pomocí biometrických údajů, elektronického podpisu, mobilního zařízení (SIM karty), na které se zasílají sms kódy, mobilního zařízení s aplikací smartbanking, nebo jiných důvěrných informací.
2. Klient je povinen oznámit ztrátu, odcizení nebo zneužití výše uvedených údajů telefonicky na tel. číslo: + 420 224 346 797. 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 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 a těchto Podmínek (včetně Ceníku) (dále také „návrh na změnu smlouvy“). Návrh na změnu smlouvy se klientovi poskytuje alespoň 2 měsíce před navrženou účinností změny smlouvy, a to prostřednictvím internetbankingu, pokud ho má klient zřízený, nebo na jiném trvalém nosiči dat, anebo osobně na pobočce banky, která klientovi vede účet. Platí (smluvní strany se tak dohodly), že klient návrh na změnu smlouvy přijal, jestliže (i) byl návrh poskytnut klientovi způsobem a ve lhůtě podle předchozí věty, (ii) klient návrh na změnu smlouvy neodmítl, (iii) banka o tomto důsledku klienta v návrhu informovala a (iv) banka v návrhu na změnu smlouvy informovala klienta o jeho právu bezúplatně a s okamžitou účinností vypovědět smlouvu přede dnem, kdy má navrhovaná změna nabýt účinnosti, pokud klient takový návrh odmítne. Pokud klient návrh na změnu smlouvy odmítne, má právo smlouvu přede dnem, kdy má změna smlouvy nabýt účinnosti, bezúplatně a s okamžitou účinností vypovědět. Jestliže klient odmítne návrh na změnu smlouvy a nevyužije svého práva dle předchozí věty, považuje se to automaticky za výpověď smlouvy podanou bankou, pokud nestanoví banka jinak. Odmítnutí návrhu na změnu smlouvy, odvolání odmítnutí návrhu na změnu smlouvy nebo výpověď smlouvy musí být v písemné podobě a v souladu s čl. XVII odst. 2 Podmínek doručena na adresu sídla banky nebo na jakoukoliv pobočku banky. Klient je kdykoli oprávněn po dobu výpovědní lhůty odvolat svoje odmítnutí návrhu na změnu smlouvy. Včasné odvolání odmítnutí návrhu na změnu smlouvy, dle předchozí věty, má za následek, že podaná výpověď se považuje za zrušenou. Klient žádá banku, aby mu byl návrh na změnu smlouvy zaslán do internetbankingu nebo na jiném trvalém nosiči dat v podobě nového úplného znění smlouvy nebo Podmínek tak, aby mohl tento návrh uchovat a využívat po přiměřenou dobu a mohl tento návrh v nezměněné podobě reprodukovat. V případě, že nemá klient zřízen internetbanking, žádá klient banku, aby mu byl návrh na změnu smlouvy poskytnut osobně na pobočce banky, kde uzavřel příslušnou smlouvu v podobě nového úplného znění smlouvy nebo Podmínek v písemné podobě tak, aby mohl tento návrh uchovat a využívat po přiměřenou dobu a mohl tento návrh v nezměněné podobě reprodukovat. Banka žádost klienta přijímá.
2. V případě, že klient nepodepíše odmítnutí návrhu na změnu smlouvy, odvolání odmítnutí návrhu na změnu smlouvy, výpověď smlouvy či jakýkoliv jiný dokument, jehož důsledkem je změna či zánik smlouvy, před pracovníkem banky, je povinen svůj podpis na takovém dokumentu úředně ověřit.
3. Tyto Podmínky byly vyhlášeny dne 21.4.2015, nabývají účinnosti dnem 22.6.2015 a k témuž dni nahrazují veškeré dosavadní Podmínky.

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