Obchodní podmínky pro elektronickou správu účtů

vedených bankou Fio banka, a.s., IČO: 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 též 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“). Do internetbankingu se oprávněná osoba přihlašuje za použití svého přihlašovacího jména a přístupového hesla, případně i dalšího Bankou požadovaného údaje či bezpečnostního prvku (např. SMS kódu či smartbankingu). 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. Při udělení zmocnění určí majitel účtu i rozsah zmocnění, tj. které úkony je zmocněná osoba oprávněna činit. Zmocněnec používá způsob autorizace elektronické komunikace tak, jak ho má domluven s bankou.
2. Tyto Obchodní podmínky pro elektronickou správu účtů (dále jen „Podmínky“ nebo „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. 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 služby Internetbanking) 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 vlivu klienta, zabezpečení zařízení klienta", odst. 1 Podmínek. 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. Není-li dále uvedeno jinak, elektronicky podané pokyny musí být klientem autorizovány pomocí bezpečnostního prvku, tj. podepsány jedním z dále uvedených způsobů, nebo jejich kombinací, v závislosti na způsobu zvoleném klientem, případně stanoveném bankou v čl. VIII Podmínek. Banka je oprávněna způsoby autorizace elektronicky podaných pokynů i jednostranně měnit, tj. je oprávněna požadovat autorizování pokynů i způsobem, který nemusí být popsán v těchto podmínkách. 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 použitím zabudovaného biometrického snímače. Jestliže byl pokyn autorizován (ať již s využitím bezpečnostního prvku nebo bez využití bezpečnostního prvku dle odst. 1c. až 1e tohoto čl. III. Podmínek), má se za to, že klient souhlasil s podáním a provedením pokynu, pokud není klientem prokázáno, že pokyn neautorizoval. Práva a povinnosti klienta dle tohoto čl. III. Podmínek se obdobně použijí na osobu oprávněnou klientem k elektronické správě jeho účtu, není-li výslovně uvedeno jinak. V souladu s předchozí větou se tedy způsob autorizace (včetně možnosti podávat pokyny bez autorizace pomocí bezpečnostního prvku) může u jednotlivých osob oprávněných nakládat se zůstatkem stejného účtu lišit, a klient jako majitel účtu již na nastavení způsobu autorizace pokynů dalších jím oprávněných osob nemá vliv.

1a. Pokud je bankou a klientem (či osobou oprávněnou podávat či autorizovat pokyny za klienta) domluven způsob autorizace elektronicky podávaných pokynů (prostřednictvím internetbankingu), rozumí se tím stanovení způsobu autorizace pokynů s využitím některého z bankou využívaných bezpečnostních prvků (např. sms autorizační kód, elektronický podpis či jejich kombinace), avšak pouze ve vztahu k těm pokynům, u nichž banka autorizaci s využitím některého bezpečnostního prvku vyžaduje; banka je oprávněna pro některé druhy pokynů nevyžadovat autorizaci s využitím bezpečnostního prvku, a to za podmínek stanovených v těchto Podmínkách (může se jednat o druhy pokynů, kdy pro takový postup není třeba speciálního úkonu ze strany klienta, i o druhy pokynů, kdy takový postup musí klient nejdříve autorizovat s využitím používaného bezpečnostního prvku). Umožňuje-li to banka, klient je oprávněn pokyny podané prostřednictvím internetbankingu autorizovat klientem zvoleným způsobem autorizace také prostřednictvím smartbankingu.

1b. **Elektronicky podané pokyny, které nemusí být klientem autorizovány pomocí bezpečnostního prvku.** Za podmínek vymezených v odst. 1c, 1d a 1e tohoto čl. III. Podmínek a ode dne, kdy banka umožňuje či umožní takový způsob provádění elektronicky podaných pokynů, je klient oprávněn provést bez využití bezpečnostního prvku následující typy elektronicky podaných pokynů:

- pokyn k převodu z účtu klienta na jiný účet téhož klienta vedený bankou (dále též jen „převod mezi účty klienta“),
- pokyn k převodu malé částky z účtu klienta (dále též jen „převod malé částky“),

- pokyn k převodu z účtu klienta na účet dle prověřené šablony (dále též jen „převod dle prověřené šablony“).

Klient je oprávněn podat a autorizovat prostřednictvím internetového bankovnictví pokyn k povolení provádění jednotlivého typu převodů bez autorizace pomocí bezpečnostního prvku. Banka je oprávněna (ne však povinna) ode dne, kdy umožní výše uvedené typy elektronicky podaných pokynů provádět bez autorizace pomocí bezpečnostního prvku (tj. ode dne zahájení takové služby), automaticky povolit klientovi provádění jednotlivého typu takových převodů i bez předchozího pokynu klienta k takovému povolení. Klient je oprávněn podat prostřednictvím internetového bankovnictví pokyn (který není autorizován pomocí bezpečnostního prvku) k zakázání provádění jednotlivého typu převodů bez autorizace pomocí bezpečnostního prvku. Pokud klient zakázal provádění převodů bez autorizace pomocí bezpečnostního prvku, takové převody musí být klientem standardně autorizovány pomocí bezpečnostního prvku dle odst. 1 tohoto článku. I pokud má klient povoleno provádění převodů bez autorizace pomocí bezpečnostního prvku, banka je vždy oprávněna u jednotlivého pokynu vyžadovat jeho autorizaci pomocí bezpečnostního prvku. Přehled nastavených autorizací je uveden v internetovém bankovnictví v sekci „Nastavení“.

1c. **Převod mezi účty klienta.** Klient je oprávněn (za podmínek dle odst. 1b. tohoto článku) provést bez autorizace pomocí bezpečnostního prvku elektronický pokyn k převodu částky z účtu klienta na jakýkoli jiný účet téhož klienta vedeného bankou (majitelem účtu plátce a účtu příjemce musí být tedy totožná osoba).

1d. **Převod malé částky.** Klient je oprávněn (za podmínek dle odst. 1b. tohoto článku) provést bez autorizace pomocí bezpečnostního prvku elektronický pokyn malé částky z účtu klienta, a to do výše limitů stanovených bankou. Banka je oprávněna stanovit limit pro maximální výši částky jednotlivého převodu bez autorizace pomocí bezpečnostního prvku až do 30 eur (resp. ekvivalentu v CZK), limit pro maximální kumulativní výši po sobě jdoucích převodů bez autorizace pomocí bezpečnostního prvku až do 100 eur (resp. ekvivalentu v CZK) od posledního pokynu autorizovaného pomocí bezpečnostního prvku a limit pro maximální počet po sobě jdoucích převodů bez autorizace pomocí bezpečnostního prvku až do počtu pět od posledního pokynu autorizovaného pomocí bezpečnostního prvku. Je-li podáním elektronického pokynu překročen jakýkoli limit stanovený bankou, takový pokyn je klient povinen standardně autorizovat pomocí bezpečnostního prvku dle odst. 1 tohoto článku. Elektronicky podaný pokyn v jiné méně než CZK bude pro účely tohoto odst. 1d. přepočten aktuálním kurzem ČNB.

1e. **Převod dle prověřené šablony.** Klient je oprávněn (za podmínek dle odst. 1b. tohoto článku) provést bez autorizace pomocí bezpečnostního prvku elektronický pokyn k převodu částky dle šablony, kterou klient označí v internetovém bankovnictví nebo, umožňuje-li to banka, ve smartbankingu za prověřenou (pro účely těchto Podmínek též jen „prověřená šablona“). Klient bere na vědomí a souhlasí, že se bez autorizace pomocí bezpečnostního prvku provede i elektronický pokyn, který nebyl zadán s využitím prověřené šablony, pokud se parametry tohoto elektronického pokynu shodují se všemi parametry nastavenými klientem v rámci prověřené šablony, s výjimkou částky (prověřená šablona musí mít nastavený alespoň účet příjemce, ostatní parametry jsou nepovinné); pokud je u prověřené šablony nastavena částka (tj. měsíční limit), uplatní se takový limit i pro takto podávaný pokyn. Pokud není v rámci prověřené šablony nastaven účet plátce, platí, že prověřenou šablonu je oprávněn použít klient pro jakýkoli účet, který je oprávněn samostatně elektronicky spravovat, nestanoví-li banka jinak. Pokud je v rámci prověřené šablony nastaven účet plátce, platí, že prověřenou šablonu je oprávněna použít jakákoli osoba, která je oprávněna elektronicky spravovat účet plátce, nestanoví-li banka jinak. Klient je oprávněn stanovit si v internetovém bankovnictví nebo, umožňuje-li to banka, ve smartbankingu měsíční limit pro provádění takových převodů bez autorizace pomocí bezpečnostního prvku (měsíční limit se nastavuje uvedením částky v rámci prověřené šablony; pokud měsíční limit není uveden, platí, že prověřená šablona je nastavena s neomezeným měsíčním limitem, nestanoví-li banka jinak). Je-li podáním elektronického pokynu překročen tento limit, takový pokyn je klient povinen standardně autorizovat pomocí bezpečnostního prvku dle odst. 1 tohoto článku.

2. Autorizace elektronickým podpisem. Banka dodá klientovi program, který mu umožní vytvořit si vlastní elektronický podpis – klíč. Klient je oprávněn po započetí elektronické komunikace změnit klíč. Změnu klíče provede klient tak, že v programu dodaného mu bankou si vytvoří nový klíč, jehož veřejnou část osobně předá bance na její pobočce. V případech, kdy banka prostřednictvím internetbankingu vyzve klienta ke změně klíče, je klient povinen tuto změnu provést ve lhůtě uvedené ve výzvě. V opačném případě banka klíč po marném uplynutí lhůty zruší. Po zrušení klíče nebude klient moci provádět pokyny, které vyžadují autorizaci dle čl. VIII odst. 9 Podmínek, a to do doby, dokud neprovede změnu klíče výše uvedeným způsobem. Veřejnou část svého klíče předá klient osobně před započetím elektronické komunikace bance. Správa přístupu k tajné části 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 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 potvrzením pokynu (odkliknutím dané volby) v elektronické aplikaci Fio-podpis, přičemž před prvním potvrzením pokynu je potřeba uvést své heslo k soukromé části klíče do elektronické aplikace Fio - podpis. Klient má povinnost odhlásit se z elektronické aplikace Fio – podpis vždy bezprostředně po ukončení práce s ní a nikdy neponechávat mimo dohled své zařízení, pokud je klient přihlášen do elektronické aplikace Fio - podpis.

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 (včetně tzv. hromadného pokynu k více transakcím, apod.). 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. 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. Není-li dále stanoveno jinak, 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. Umožňuje-li banka zřízení přístupu do smartbankingu prostřednictvím QR kódu, klient zřídí přístup do smartbankingu výhradně následujícím způsobem: i) klient zadá (a autorizuje) pokyn v internetbankingu pro vygenerování QR kódu (jednorázový kód s omezenou platností); tento pokyn musí být řádně autorizován elektronickým podpisem a/nebo jednorázovým sms kódem v závislosti na způsobu autorizace zvolené klientem, ii) klient použije vygenerovaný QR kód nebo číselný kód ve smartbankingu pro spárování zařízení, iii) klient si ve smartbankingu zřídí přístupové heslo do smartbankingu a případně také PIN pro autorizaci pokynů prostřednictvím smartbankingu. 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 (prostřednictvím svého přístupového hesla nebo použitím biometrického snímače použitého na spárovaném mobilním zařízení).

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 použitím zabudovaného biometrického snímače. Banka je oprávněna požadovat autorizaci PINem pro smartbanking i v případě, má-li klient zvolenu autorizaci za použití 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 (umožňuje-li banka takový způsob autorizace) 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 dle postupu uvedeného v odst. 3a tohoto článku (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. 1c. až 1e. a odst. 3a může klient změnit elektronicky prostřednictvím internetového rozhraní internetbankingu, nestanoví-li banka jinak. Způsob a podmínky autorizace dle odst. 3a (umožňuje-li to banka) a 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 také 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 v čl. VIII.

Čl. VI. Rozsah odpovědnosti stran

1. Klient odpovídá za závazky vzniklé elektronickým podáním pokynu stejně, jako by byly pokyn nebo žádost podány 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 či smartbankingu, porušení povinností k zabezpečení mobilního zařízení/SIM karty používané pro zasílání SMS kódů, porušení povinnosti ověřit adresu serveru banky, porušení povinnosti ověřit identifikaci aplikace pro elektronický podpis, porušení povinnosti řádně zkontrolovat pomocí zeleného symbolu visacího zámku následovaného názvem „Fio banka, a.s. (CZ)“ nebo zeleného nápisu Fio banka v adresním řádku internetového prohlížeče, že komunikuje se serverem banky 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. Neuplatní-li se odpovědnost dle čl. VI. odst. 3 Podmínek, klient, který je spotřebitelem, nese ztrátu za veškeré neautorizované (neoprávněné) platby i) uskutečněné do 12.1.2018 (včetně) do částky odpovídající 150 EUR, nebo ii) uskutečněné od 13.1.2018 do částky odpovídající 50 EUR, byla-li tato ztráta způsobena v důsledku zneužití internetbankingu či smartbankingu z důvodu nezajištění ochrany osobních (personalizovaných) bezpečnostních prvků (zejména přihlašovací jméno, heslo, autorizační sms kód, apod.). Klient, který není spotřebitelem, nese ztrátu za veškeré neautorizované platby uskutečněné v důsledku zneužití internetbankingu či smartbankingu z důvodu nezajištění ochrany osobních bezpečnostních prvků v plném rozsahu.
6. Pro odpovědnost banky se dále použijí ustanovení odst. 29 až 32 čl. XIII. Obchodních podmínek pro zřizování a vedení účtů, vydaných bankou.

Čl. VII. Smluvní odměna a poplatky

1. Výše odměny účtovaná bankou za umožnění elektronické správy účtů je uvedena v Ceníku finančních operací a služeb (dále též jen „Ceník"), 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, podávat zejména 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,
   - zřízení/zrušení tokenu pro službu API,
   - 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 SMS a emailového upozornění 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,
   - povolení/zakázání provádění pokynů uvedených v odst. 1b. čl. III Podmínek bez autorizace pomocí bezpečnostního prvku a případně s tím související další pokyny,
   - změna UID mobilního zařízení pro smartbanking,
   - změna způsobu a frekvenci předávání výpisů z účtů,
   - uzavření Smlouvy o vydání platební karty a dalších smluv dle aktuální nabídky banky,
   - umožňuje-li to banka, uzavření dodatků k dříve uzavřeným smlouvám,
   - 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),

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

- zadání/změna/zrušení korespondenční adresy,
- zadání/zrušení kontaktního telefonu,
- zadání/zrušení kontaktního e-mailu,
- změna pobočky, na které je evidovaná dokumentace klienta.

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. Banka je oprávněna (ne však povinna) některé pokyny uvedené v tomto čl. VII umožnit podat a autorizovat také nezletilým klientům (jedná se např. o pokyny či požadavky související s SMS a emailovým upozorněním, vydanou platební kartou k danému účtu či smartbankingem); banka je oprávněna rozsah pokynů, které lze podat a autorizovat nezletilým klientem, dle vlastního uvážení rozšířit i zúžit.
10. Elektronickou správou účtů lze zadat požadavek na založení nebo zrušení SMS a emailového upozornění o některých událostech na účtu. Klient si může zvolit upozornění 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. Banka je oprávněna (ne však povinna) i bez předchozího upozornění jednostranně zrušit SMS a emailové upozornění, pokud dojde ke vzniku neoprávněného debetního zůstatku na účtu klienta; po vyrovnání debetního zůstatku se SMS a emailové upozornění neobnovuje - pro obnovení služby je potřeba nové založení SMS a emailového upozornění, které může klient provést po vyrovnání debetního zůstatku.
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 karty, jejíž kredit má být převodem dobit, případně určí i příslušného mobilního operátora (je-li to vyžadováno) a zadá jiné bankou požadované údaje.
12. Banka si vyhrazuje právo omezit dispozici s peněžními prostředky na účtu (popř. s určitou výší peněžních prostředků) prostřednictvím internetbankingu či smartbankingu, a to zejména z důvodu výkonu rozhodnutí či z důvodu exekuce. Pokud je dispozice s peněžními prostředky na účtu dle předchozí věty omezena a majitel účtu má zákonný nárok na výplatu peněžních prostředků (např. nárok na výplatu dvojnásobku životního minima), banka je oprávněna, ne však povinna, zamezit jejich vyplacení prostřednictvím internetbankingu či smartbankingu a vyžadovat, aby majitel účtu tento nárok uplatnil na pobočce banky; banka má však právo (ne povinnost) umožnit vyplacení takové částky i prostřednictvím internetbankingu či smartbankingu, a to i v případě, kdy účet majitele spravuje osoba odlišná od majitele účtu – pro případ takového postupu k tomu majitel účtu zmocněnou osobu ve smyslu čl. 1 odst. 1 těchto podmínek zmocňuje.
13. Není-li v těchto Podmínkách stanoveno výslovně jinak, a není-li ve zmocnění uděleném ve smyslu čl. I. odst. 1 těchto Podmínek výslovně stanoveno, že zmocnění nezaniká úmrtím majitele účtu, zmocnění udělené dle čl. I. odst. 1 těchto Podmínek zaniká desátý pracovní den po dni doručení oznámení o úmrtí majitele účtu bance; ustanovení této věty však platí pouze pro případy, kdy se banka o úmrtí klienta poprvé dověděla po 31.12.2016. Banka je však oprávněna (ne povinna) zrušit oprávnění k elektronické správě účtů ve smyslu čl. I. odst. 1 těchto Podmínek i bezodkladně po doručení oznámení o úmrtí majitele účtu bance.
14. Klient je oprávněn prostřednictvím písemné žádosti (na libovolné pobočce banky či korespondenčně s úředně ověřenými podpisy) nastavit maximální denní a měsíční limit majitele a limit příkazce (pro účely tohoto odstavce též jen „limit“) pro elektronicky podané pokyny (počáteční limit není ze strany banky nastaven) a toto nastavení následně i měnit; v takovém případě je možné elektronické pokyny podat prostřednictvím internetbankingu a smartbankingu v součtu za všechny pokyny pouze do výše aktuálně nastaveného limitu, není-li uvedeno jinak. „Limit majitele“ je limit nastavený klientovi jako majiteli účtu; tento limit platí souhrnně pro všechny účty vedené pro tohoto klienta bez ohledu na to, zda byl pokyn podán klientem nebo jakýmkoli zmocněncem. „Limit příkazce“ je limit nastavený klientovi jako uživateli internetbankingu, resp. smartbankingu; tento limit platí souhrnně pro všechny pokyny podané uživatelem bez ohledu na to, k jakému účtu byl pokyn podán. Banka je oprávněna některé typy pokynů nezapočítávat do nastaveného limitu (jedná se zejména o příkazy k inkasu, avizování výběru hotovosti či převody mezi účty klienta). Elektronicky podaný pokyn v jiné měně než CZK bude pro účely tohoto odstavce přepočten kurzem ČNB aktuálním k okamžiku podání pokynu. Banka je oprávněna nastavit konkrétnímu klientovi maximální denní a měsíční limit i bez jeho výslovné žádosti (zejména v případě nezletilých osob nebo opatrovnictví); výše takových limitů je stanovena bankou. Maximální výše denního limitu i měsíčního limitu v případě nezletilého klienta je 15.000,- Kč; banka je oprávněna stanovené limity individuálně změnit. Maximální výši limitu stanoveného bankou pro nezletilého klienta je oprávněn klient změnit po nabytí zletilosti, resp. plné svéprávnosti prostřednictvím písemné žádosti na libovolné pobočce banky. Banka si vyhrazuje právo jednostranně měnit limity uvedené v tomto odstavci, včetně snížení nastavených limitů, a to i individuálně ve vztahu ke konkrétnímu klientovi. Důvodem případného individuálního snížení limitů ze strany banky může být zejména porušení smlouvy, těchto podmínek, výkon rozhodnutí nebo exekuce, vydání rozhodnutí dle insolvenčního zákona o způsobu řešení úpadku klienta, zvýšení rizika neschopnosti splácení závazků klientem, apod. Po pominutí původních důvodů pro snížení limitu je banka oprávněna, ne však povinna, i bez žádosti klienta upravit limity na hodnoty platné před jejich snížením ze strany banky.

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, e-PIN (pro platby kartou), telefonní číslo, UID mobilního zařízení, kód

(passcode, PIN) pro přístup k mobilnímu zařízení, token pro službu API 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, které je používáno pro přihlášení do internetbankingu, smartbankingu 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, informace o pohybech, účtech atd.), která jsou přenášena mezi zařízením klienta a serverem Fio. Veškerá přenášená data jsou šifrována standardizovanými algoritmy s minimálně 128 bitovými klíči. 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 jsou uvedeny také na přihlašovací stránce do internetbankingu.

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, není-li dále uvedeno jinak. Klient si může změnit heslo pouze v internetbankingu či smartbankingu, umožňuje-li to banka. 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, není-li dále uvedeno jinak. Vyprší-li tato lhůta, bude klient při nejbližším přihlášení do internetbankingu či smartbankingu vyzván k jeho změně. Má-li klientovo aktuální heslo do internetbankingu či smartbankingu alespoň 12 znaků, banka je oprávněna (nikoli však povinna) považovat takové heslo za platné i poté, co uplyne doba platnosti takového hesla dle tohoto odstavce, a to až na dobu neomezeně dlouhou. V takovém případě klient nebude po přihlášení do aplikace internetbanking či smartbanking vyzván ke změně hesla. Banka doporučuje, aby klient nepoužíval pro různé aplikace (zejména internetbanking a smartbanking, ale i jiné typy aplikací, jako např. e-mailová schránka, sociální sítě, hry apod.)

stejná přístupová hesla, zejména aby taková shoda hesel nebyla mezi aplikací s přístupem k účtu a jakoukoli jinou používanou aplikací.

6. Klient má povinnost dodržovat dostatečnou míru obezřetnosti při zadávání důvěrných údajů, zejména nezasílat důvěrné údaje pomocí e-mailu, sms, sociálních sítí (např. Facebook, Twitter, LinkedIn) či aplikací pro vzájemnou komunikaci (např. Skype, ICQ), nezadávat je na jiné internetové stránce, než na stránce určené k přihlášení do internetbankingu, a to ani v případě, že klient obdrží e-mail, sms či zprávu, 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 a tokenu pro službu API

1. Prostřednictvím tokenu pro službu API je klient, resp. osoba disponující tokenem pro službu API, oprávněn získávat informace o účtu, zadávat pokyny k úhradě (ne však takové pokyny autorizovat) nebo činit jiné úkony bez přihlášení do internetového bankovnictví (bez uvedení přihlašovacího jména a přístupového hesla). Bližší informace o službě API a tokenu pro službu API jsou uvedeny na internetových stránkách banky. Klient má povinnost chránit svůj elektronický klíč, který používá při autorizaci pokynů, a token pro službu API proti jeho zneužití, zejména proti jeho odcizení, okopírování apod. Zneužitím elektronického klíče klienta nebo tokenu pro službu API může jiná osoba předstírat identitu klienta a zadávat či autorizovat pokyny jménem klienta, popř. činit další úkony jménem klienta. Zneužití elektronického klíče nebo tokenu pro službu API může způsobit klientovi škodu. Token pro službu API k účtu klienta – fyzické osoby zaniká desátý pracovní den po dni doručení oznámení o úmrtí klienta bance; ustanovení této věty však platí pouze pro případy, kdy se banka o úmrtí klienta poprvé dověděla po 31.12.2016. Banka je však oprávněna (ne povinna) zrušit token pro službu API k účtu klienta – fyzické osoby i bezodkladně po doručení oznámení o úmrtí majitele účtu bance.
2. Klient má povinnost elektronický klíč a token pro službu API uchovávat pouze na zabezpečeném místě (např. počítač, server, přenosné médium atd.), na kterém si může být s dostatečnou mírou jist, že je chráněn proti možným hrozbám plynoucím z připojení k datové síti. Klient má povinnost uchovávat elektronický klíč pouze na zašifrovaném disku nebo elektronický klíč zašifrovat. Klient nesmí uchovávat a používat elektronický klíč a token pro službu API na místě, které je volně (bez vědomí či povolení klienta) přístupné třetím osobám.
3. Pokud klient uchovává elektronický klíč nebo token pro službu API na přenosném médiu, klient má povinnost ukládat toto médium na místo, kde je do velké míry omezeno riziko jeho zneužití, zejména odcizení, okopírování nebo poškození.
4. Rozsah odpovědnosti stran je vymezen v čl. VI. těchto Podmínek. Klient je vždy odpovědný za způsobenou škodu v souvislosti s použitím tokenu pro službu API třetí osobou, zejména pokud klient třetí osobě token pro službu API zpřístupnil.

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 10 tohoto článku. Všechny informace zahrnuty v odstavcích 2 až 10 tohoto článku jsou povinnosti, není-li u některé z nich výslovně uvedeno jinak.
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 má povinnost odhlásit se z internetbankingu vždy bezprostředně po ukončení práce s ním a nikdy neponechávat mimo dohled své zařízení, pokud je klient přihlášen do internetbankingu.
3. Klient má povinnost se před přihlášením do internetbankingu řádně přesvědčit, že komunikuje se správným poskytovatelem služby. Klient má povinnost vždy ověřit, že v adresním řádku prohlížeče je adresa začínající: https://ib.fio.cz/ib/, https://ib.fio.sk/ib/, https://www.fio.cz/ib2/, https://www.fio.sk/ib2/, https://www.fio.pl/ib2/, https://www1.fio.cz/ib2/, https://www2.fio.cz/ib2/ nebo https://www3.fio.cz/ib2/, a stránka používá šifrované spojení se serverem banky za použití platného certifikátu SSL serveru. Tato skutečnost je indikována pomocí zeleného symbolu visacího zámku následovaného názvem „Fio banka, a.s. (CZ)“ nebo zeleného nápisu Fio banka v adresním řádku internetového prohlížeče. Názorný příklad ověření platnosti certifikátu dle tohoto odstavce je dostupný na: https://www.fio.cz/docs/cz/sec/fingerprint.pdf. Zde je dostupný i příklad ověření identifikace serveru banky prostřednictvím tzv. SHA1 Fingerprintu (toto ověření však není povinné, i když je doporučováno). 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. Banka má právo kdykoliv omezit přístup na kteroukoli z adres uvedených v tomto odstavci, a to dočasně i trvale.
4. 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.
5. 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.
6. Klient má povinnost zabezpečit na zařízení, na kterém se rozhodne používat internetbanking a kde je to technicky možné, alespoň antivir a funkční firewall a tyto ochranné prvky pravidelně aktualizovat. Klient má povinnost pravidelně sledovat na stránkách banky (viz. čl. XI. odst. 3 Podmínek) informace o nových hrozbách nebo ve zprávách v internetbankingu, popř. smartbankingu a je povinen se podle poskytnutých informací chovat, včetně povinnosti aktualizovat operační systém na zařízení, na kterém používá internetbanking. Klient je povinen číst varovná oznámení a upozornění, která mu banka zašle prostřednictvím e-mailu nebo sms. Pokud varovné oznámení nebo upozornění zaslané bankou dle předchozí věty obsahuje informaci, které klient nerozumí, nebo obsahuje popis činnosti, kterou klient neprováděl nebo si klient není jist, zda takovou činnost prováděl, nebo obsahuje jinou informaci vzbuzující podezření, že došlo k neoprávněné manipulaci s účtem, nebo obsahuje přímo výzvu ke kontaktování banky, je klient povinen kontaktovat banku za použití ověřitelných kontaktních údajů

banky (přednostně na telefonní číslo +420 224 346 392). Banka ve varovném oznámení a upozornění zasílaném prostřednictvím e-mailu nebo sms nebude z bezpečnostních důvodů uvádět své konkrétní kontaktní údaje.

7. Klient je povinen pro přístup do internetbankingu používat důvěryhodný internetový prohlížeč, který pravidelně aktualizuje. Klient je povinen neměnit výchozí zabezpečení internetového prohlížeče na zabezpečení méně bezpečné. Klient je povinen kontrolovat vždy před zadáním přihlašovacích údajů na přihlašování stránce internetbankingu, zda prohlížeč nehlásí jakékoli varování spojené s certifikátem (vypršelý nebo nedůvěryhodný certifikát nebo certifikát vydaný pro jinou instituci než banku). Postup pro zjištění podrobností týkajících se certifikátu je dostupný na: https://www.fio.cz/docs/cz/sec/fingerprint.pdf.
8. Klient má povinnost vyvarovat se používání internetbankingu na operačních systémech a prohlížečích, které daný výrobce již nepodporuje. Klient má povinnost udržovat operační systém zařízení, na kterých používá internetbanking, a používaný internetový prohlížeč s nejnovějšími nainstalovanými aktualizacemi od výrobce. Klient je povinen nepoužívat internetbanking na zařízeních využívajících verze operačního systému Windows XP a starší.
9. Klient má povinnost na zařízeních, na kterých používá internetbanking, vyvarovat se stahování nedůvěryhodných souborů a instalování nedůvěryhodných programů. Klient má povinnost na zařízení, na kterém využívá internetbanking, navštěvovat pouze známé, důvěryhodné a bezpečné stránky na internetu a neotevírat přílohy doručených e-mailů s podezřelým předmětem, odesílatelem nebo obsahem (textem e-mailu) na takovém zařízení; výčet některých relevantních indicií je uveden v odstavci 12 tohoto článku - jedná se však pouze o demonstrativní výčet a při posuzování podezřelosti e-mailu se klient nesmí omezit pouze na tam uvedené indicie. Klient má povinnost nepoužívat k přístupu do internetbankingu odkazů otevíraných ze sociálních sítí, e-mailů, sms či aplikací pro vzájemnou komunikaci. Banka nebude v žádném případě zasílat odkazy na stránku určenou k přihlášení do internetbankingu prostřednictvím sociálních sítí, e-mailů, sms či aplikací pro vzájemnou komunikaci. Banka doporučuje, aby klient používal ve své emailové schránce spam filtr (používání spam filtru snižuje pravděpodobnost obdržení e-mailu, který obsahuje vir či jiný škodlivý obsah).
10. Na vyspělejším mobilním zařízení (zejména tzv. smartphony a tablety) s operačním systémem iOS, Android, Windows Phone a jiným operačním systémem, na kterých se používá internetbanking, smartbanking nebo SIM karta obsahující telefonní číslo určené k přijímání autorizačních sms kódů od banky, je klient povinen 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.
11. 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.
12. Podezřelé či falešné e-maily, ve kterých podvodníci předstírají jednání banky nebo jiného subjektu, mohou být indikovány například tím, že:
    a) obsahují odkaz na internetovou stránku, kde název odkazu nekoresponduje se skutečnou adresou internetových stránek (po umístění kurzoru myši nad odkaz se ukáže skutečná internetová adresa),
    b) obsahují výzvu vyžadující okamžité jednání adresáta (např. zaplacení poplatku, instalaci aplikace, hrozbu exekuce na majetek, pokud se okamžitě neuhradí atd.),
    c) obsahují v textu e-mailu zjevné gramatické a pravopisné chyby,
    d) obsahují neurčité či nedůvěryhodné kontaktní údaje odesílatele,
    e) obsahují text v neočekávaném jazyce (např. e-mail od exekutora v anglickém jazyce),
    f) nabízejí velmi výhodné podmínky, výdělky, odměny, půjčky či investice, velmi levné zboží atd.,
    g) v případě e-mailu zaslaného údajně bankou obsahuje takový e-mail přílohy typu .exe, .zip, .rar, .ppt atd. (takové přílohy banka nezasílá),
    h) vyzývají k zadání osobních údajů klienta, hesla nebo PINu, nebo
    i) v e-mailu je přímo proklik na vstupní formulář internetového bankovnictví.

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“). Banka odesílá autorizační sms kódy na takto určené telefonní číslo, za samotné doručení autorizačního sms kódu však nenese odpovědnost a tedy neodpovídá ani za případnou škodu klienta vzniklou nedoručením autorizačního sms kódu. Klient je povinen používat k přijímání autorizačních sms kódů takovou SIM kartu, na kterou je možno bezproblémově doručovat SMS zprávy odesílané prostřednictvím mobilních operátorů poskytujících legálně služby na území České republiky; plnění této povinnosti však banka nekontroluje a důsledek jejího případného porušení jde plně k tíži klienta. Banka zejména upozorňuje, že v případě přijímání autorizačních sms kódů prostřednictvím SIM karty zahraničního operátora existuje zvýšené riziko nedoručení autorizačních sms kódů na takovou SIM kartu.
2. Klient má povinnost bránit zneužití mobilního zařízení či SIM karty a přijmout veškerá opatření k jejich ochraně.
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, na kterém klient využívá aplikaci smartbanking. 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. Klient má povinnost zabezpečit na mobilním zařízení, na kterém se rozhodne používat internetbanking nebo smartbanking a kde je to technicky možné, alespoň antivir a funkční firewall a tyto ochranné prvky pravidelně aktualizovat. Banka doporučuje, aby klient používal na mobilních zařízeních, která to umožňují a prostřednictvím kterých využívá služeb banky, aplikaci smartbanking namísto přihlašování do internetbankingu prostřednictvím internetových prohlížečů.
9. 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 zabezpečit takové mobilní zařízení, pokud je to technicky možné, alespoň funkčním firewallem a antivirovou ochranou a tyto ochranné prvky pravidelně aktualizovat.
10. Klient má povinnost pravidelně sledovat informace (zejména od banky) o nových hrozbách, virech, spyware apod. a v souladu s tím zajistit ochranu mobilního zařízení.
11. Postup uvedený v odstavcích 8 až 10 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.
4. Pokud banka po zablokování internetbankingu, smartbankingu nebo použití biometrického snímače pro aplikaci smartbanking kontaktuje klienta, banka ho kontaktuje bankou zvoleným způsobem (například telefonicky nebo elektronicky), a v takovém případě mu oznámí důvody blokace a dohodne s ním další postup, např. změnu z dočasné blokace na trvalou blokaci.

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, tokenu pro službu API nebo jiných důvěrných informací.
2. Klient je povinen oznámit ztrátu, odcizení nebo zneužití výše uvedených údajů telefonicky na tel. číslo: +420 224 346 392. Tato telefonní linka je klientovi k dispozici nepřetržitě kterýkoliv den v roce. Při oznámení je klient povinen zodpovědět kontrolní otázky položené bankou. Bez sdělení těchto údajů se nepovažuje oznámení klienta za řádné a banka není povinna takové oznámení přijmout. Klient nesmí sdělit bance své heslo pro přihlášení do internetbankingu; banka nebude po klientovi požadovat sdělení hesla pro přihlášení do internetbankingu. 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.
3. Klient je povinen poskytnout bance veškerou součinnost v souvislosti s oznámením o zneužití internetbankingu nebo smartbankingu učiněného dle tohoto článku, a to zejména za účelem zjištění způsobu či příčiny napadení zařízení klienta. Klient je povinen zodpovědět otázky položené bankou, které dle názoru banky souvisejí s oznámením klienta o možném zneužití internetbankingu nebo smartbankingu. Klient je povinen na žádost banky předat zařízení, prostřednictvím kterého došlo (nebo mohlo dojít) ke zneužití internetbankingu nebo smartbankingu nebo k vyzrazení některé z informací uvedených v odstavci 1 tohoto článku, příslušnému orgánu (zejména policii) nebo bankou zvolenému nestrannému odborníkovi za účelem prozkoumání zařízení. Z tohoto důvodu je klient povinen zdržet se jakýchkoli zásahů do zařízení po zjištění možného zneužití internetbankingu nebo smartbankingu či možného vyzrazení některé z informací uvedených v odstavci 1 tohoto článku. Banka doporučuje klientovi před předáním zařízení zálohovat veškerý (resp. pro klienta podstatný) obsah zařízení.

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. 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; v takovém případě se za okamžik doručení výpovědi klientovi považuje doručení (ze strany klienta) odmítnutí návrhu na změnu smlouvy a výpovědní doba 2 měsíce začíná běžet následující den. 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 přede dnem, kdy má navrhovaná změna smlouvy nabýt účinnosti, oprávněn odvolat svoje odmítnutí návrhu na změnu smlouvy. Včasné odvolání odmítnutí návrhu na změnu smlouvy, dle předchozí věty, má za následek, že automaticky podaná výpověď ze strany banky dle předchozích ustanovení tohoto odstavce se považuje za zrušenou (neuplynula-li již výpovědní doba automaticky podané výpovědi). 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. 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. V případě sporu ze smlouvy či v souvislosti s ní je možné využít mimosoudního řešení sporu prostřednictvím služeb Finančního arbitra České republiky, Legerova 1581/69, 110 00 Praha 1, www.finarbitr.cz. Působnost Finančního arbitra České republiky je uvedena v § 1 odst. 1 zákona č. 229/2002 Sb. (v čase aktualizace tohoto dokumentu je působnost Finančního arbitra České republiky vymezena mimo jiné takto: „K rozhodování sporu spadajícího jinak do pravomoci českých soudů je příslušný též Finanční arbitr České republiky, jedná-li se o spor mezi spotřebitelem a a) poskytovatelem platebních služeb při poskytování platebních služeb, b) věřitelem nebo zprostředkovatelem při nabízení, poskytování nebo zprostředkování spotřebitelského úvěru nebo jiného úvěru, zápůjčky, či obdobné finanční služby, c) pojistitelem nebo pojišťovacím zprostředkovatelem při nabízení, poskytování nebo zprostředkování životního pojištění.“). V případech, kdy není dána působnost Finančního arbitra České republiky, a jednalo by se o případný spor vyplývající ze smluvního vztahu mezi bankou a spotřebitelem, je možné využít mimosoudního řešení sporu prostřednictvím služeb České obchodní inspekce, Štěpánská 567/15, 120 00 Praha 2, www.coi.cz. Výše uvedená mimosoudní řešení sporů mohou uplatnit pouze spotřebitelé ve smyslu zákona č. 634/1992 Sb. o ochraně spotřebitele, ve znění pozdějších předpisů.
4. Informace o zpracování osobních údajů jsou uvedeny v Informačním memorandu banky, jehož aktuální znění je klientovi dostupné na webu https://www.fio.cz/o-nas/dokumenty-ceniky/informacni-materialy případně na libovolném klientském pracovišti banky.
5. Banka a klient se dohodli, že banka vyvine snahu archivovat všechny informace a dokumenty týkající se i ukončeného smluvního vztahu mezi bankou a klientem, a to za podmínky, že
   a) již v souladu s příslušnými postupy nepřistoupila ke skartaci daných dokumentů či informací, a
   b) mezi bankou a klientem existuje jakýkoli další smluvní vztah.
6. Banka se zavazuje postupovat dle předchozího odstavce tohoto článku tak, aby dle možnosti byly všechny dotčené informace a dokumenty skartovány až najednou spolu s dokumenty a informacemi vztahujícími se k poslednímu smluvnímu vztahu, u něhož nejsou splněny podmínky pro další archivaci dle předchozího odstavce.
7. Pro účely předchozích dvou odstavců tohoto článku se smluvním vztahem nerozumí takový smluvní vztah, na základě kterého banka poskytuje klientovi pouze některou (či některé) z investičních služeb (pro tyto účely včetně případných úvěrů využívaných za účelem umožnění obchodu s investičním nástrojem).
8. Banka upozorňuje klienta, že veškerá telefonická komunikace mezi bankou a klientem je zaznamenávána. Technickou realizaci zaznamenávání telefonické komunikace pro banku v případě vybraných mobilních telefonních čísel banky zajišťuje mobilní operátor, společnost O2 Czech Republic, a.s., IČO: 60193336, se sídlem Za Brumlovkou 266/2, 14022 Praha-Michle, přičemž klient přijetím těchto obchodních podmínek vyjadřuje s takovým zaznamenáváním svůj souhlas ve smyslu § 89 odst. 1 zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů.
9. Tyto Podmínky byly vyhlášeny dne 16. 8. 2019. Obchodní podmínky nabývají účinnosti dnem 19. 8. 2019 a ke stejnému dni nahrazují dosavadní obchodní podmínky, není-li dále stanoveno jinak. Ve vztahu ke smlouvám uzavřeným před dnem účinnosti těchto obchodních podmínek podle předchozí věty, nabývají tyto obchodní podmínky účinnosti dnem 21. 10. 2019 a ke stejnému dni nahrazují dosavadní obchodní podmínky.

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

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