

SPLOŠNI POGOJI POSLOVANJA ZA POSLOVNO SPLETNO N BANKO

UVODNE DOLOČBE

1. člen

Izdajatelj teh splošnih pogojev je:

- N Banka d.d., s sedežem na naslovu Dunajska cesta 128a v Ljubljani, matična številka: 5496527, davčna številka: 41561767 (v nadaljevanju: banka),
- Banka je navedena na seznamu bank in hranilnic, ki imajo dovoljenje Banke Slovenije za opravljanje plačilnih storitev in je objavljen na spletni strani Banke Slovenije www.bsi.si,
- nadzorni organ pristojen za nadzor Banke je Banka Slovenije.

S temi splošnimi pogoji so opredeljene medsebojne pravice obveznosti in pogoji banke in uporabnika/imetnika v zvezi z uporabo Poslovne spletne N Banke.

Za vse, kar ni posebej urejeno s temi splošnimi pogoji, se uporabljajo Splošni pogoji za opravljanje plačilnih storitev preko transakcijskega računa (v nadaljevanju: Splošni pogoji za opravljanje plačilnih storitev) in vsi drugi splošni pogoji in pogodbe, ki so kakorkoli povezane ter urejajo opravljanje te storitve. V primeru neskladja med temi splošnimi pogoji in Splošnimi pogoji za opravljanje plačilnih storitev ali drugih splošnih pogojev in pogodb, ki so kakorkoli povezane ter urejajo opravljanje te storitve, veljajo določbe teh splošnih pogojev.

Ti splošni pogoji so sestavni del Okvirne pogodbe o odprtju in vodenju transakcijskega računa in Zahtevka za uporabo Poslovne spletne N Banke (v nadaljevanju: Zahtevk za uporabo), ki ga je banki podal zakoniti zastopnik imetnika transakcijskega računa in imajo značaj pogodbe.

Sestavni del teh splošnih pogojev so:

- Navodila za uporabnike Poslovne spletne N Banke (v nadaljevanju: Navodila za uporabnike spletne banke), dostopna na spletnih straneh N Banke na naslovu www.nbanka.si (v nadaljevanju: spletnih straneh banke)
- Splošne informacije o varstvu osebnih podatkov, dostopne na spletnih straneh banke: <https://www.nbanka.si/pripomocki/poti-do-banke/varstvo-osebni-podatkov/splosne-informacije-o-varstvu-osebni-podatkov>.
- Splošni pogoji storitve Rekono in njihovi sestavni deli, dostopni na www.rekono.si spletnem naslovu.

I. OPREDELITEV POJMOV

2. člen

Posamezni pojmi, uporabljeni v teh splošnih pogojih imajo naslednji pomen:

Spletna banka (v nadaljevanju tudi »EB PO«)	Je Poslovna spletna N Banka, ki je elektronski način poslovanja in opravljanja plačilnih transakcij in drugih bančnih storitev preko spletne aplikacije s strani uporabnika (fizična oseba), pooblaščenega s strani imetnika transakcijskega računa (poslovni subjekt).
Imetnik	Je imetnik transakcijskega računa, ki je poslovni subjekt in je fizična ali pravna oseba, podjetnik, zasebnik, oseba civilnega prava ali nerezident, ki ima z banko sklenjeno Okvirno pogodbo o odprtju in vodenju transakcijskega računa (poslovnega) ali Okvirno pogodbo o odprtju in vodenju e-obrestnega transakcijskega računa (v nadaljevanju: imetnik).
Zakoniti zastopnik	Je zakoniti zastopnik imetnika, ki je naveden v pristojnem registru ali katerem drugem dokumentu, ki ga izda pristojni organ.
Uporabnik	Je uporabnik Poslovne spletne N Banke in je poslovno in opravično sposobna polnoletna fizična oseba, ki jo zakoniti zastopnik imetnika, na osnovi Zahtevka za uporabo spletne banke, pooblasti za uporabo storitve spletne banke za transakcijski račun imetnika, in mu banka aktivira storitev spletne banke (v nadaljevanju: uporabnik).
Uporabniški račun	Je dostop do spletne banke za posameznega uporabnika, ki je pooblaščen za uporabo spletne banke pri enem ali več imetnikih in za uporabo uporabniškega računa uporablja svoje avtentikacijske elemente. Uporabniški račun se ustvari ob prvem vklopu storitve spletne banke uporabniku, s strani banke.
Pristopnina	Je nadomestilo, ki ga imetnik plača za vklop spletne banke na posameznem transakcijskem računu imetnika in za vklop vsakega uporabnika spletne banke na posameznem transakcijskem računu imetnika.

Mesečno nadomestilo	Je mesečni znesek, ki ga imetnik plačuje za uporabo spletne banke na posameznem transakcijskem računu. Obračunava se za vsak transakcijski račun, na katerem je pooblastilo za uporabo v spletni banki. Mesečno nadomestilo ni vezano na število uporabnikov spletne banke pri posameznemu imetniku.
Rekono storitev	<p>Rekono je družina rešitev in storitev za elektronsko identifikacijo, elektronske podpise in druge storitve zaupanja, ki omogoča varno in močno avtentikacijo, preverjanje pristnosti elektronskih dokumentov in s tem varno elektronsko poslovanje prek interneta oziroma na daljavo, oz. v okviru digitalnih bančnih poti.</p> <p>Rekono ima status kvalificiranega ponudnika storitev zaupanja, ki ga je pridobil po uspešno izvedenem postopku preverjanja s strani akreditiranega organa za ugotavljanje skladnosti, ki ga je zaključilo Ministrstvo za javno upravo z vpisom storitev zaupanja Rekono d.o.o. na nacionalni in EU seznam ponudnikov kvalificiranih storitev zaupanja.</p> <p>Uporabnik prične Rekono storitev uporabljati tako, da si ustvari Rekono račun.</p>
Rekono e-identiteta	<p>Je elektronska identiteta določene ravni zaupanja, ki jo nosi uporabnikov Rekono račun. Uporabnikova Rekono e-identiteta je lahko nizke, srednje ali visoke ravni zaupanja. Uporabnik zadostno raven zaupanja v Rekono e-identiteto za uporabo v spletni banki (tj. visoko raven) pridobi z identifikacijo v banki ali z drugimi načini, ki so možni v okviru storitve Rekono.</p> <p>V nadaljevanju teh splošnih pogojev je za Rekono e-identiteto ustrezne ravni zaupanja uporabljen poenostavljen izraz Rekono račun ustrezne ravni zaupanja.</p>
Rekono račun	<p>Uporabnik ustvari Rekono uporabniški račun (v nadaljevanju: Rekono račun), ki je nosilec uporabnikove Rekono e-identitete določene ravni zaupanja. Za uporabo v spletni banki mora imeti Rekono račun visoko raven zaupanja.</p> <p>Rekono račun je vedno vezan na uporabnika, (ki je vedno določena fizična oseba) na podlagi osebne davčne številke. Raven zaupanja v Rekono račun je odvisna od identifikacije in načina identifikacije uporabnika. Rekono račun si uporabnik ustvari neposredno na naslovu https://idp.rekono.si oz. https://www.rekono.si ali pa v postopku uporabe spletne banke. Rekono račun ustrezne ravni zaupanja se v postopku aktivacije spletne banke poveže s fizično osebo. Z Rekono računom ustrezne ravni zaupanja uporabnik tako vstopa v spletno banko.</p> <p>Uporabnik Rekono račun za uporabo z digitalnimi bančnimi potmi uporablja skladno s Splošnimi pogoji uporabe storitve Rekono in njihovim sestavnim delom, objavljenimi na https://www.rekono.si/si/kako-deluje/splosni-pogoji/ in s temi splošnimi pogoji.</p>
Avtentikacijski elementi Rekono	<p>So elementi, ki omogočajo varno avtentikacijo uporabnika pri uporabi Rekono računa v spletni banki. Ti so:</p> <ul style="list-style-type: none"> - za uporabo v spletni banki ob uporabi avtentikacije z Rekono računom: <ul style="list-style-type: none"> • e-poštni naslov (ki je uporabniško ime Rekono računa), • stalno vstopno geslo Rekono računa, • drugi faktor za avtentikacijo Rekono računa (prijava oz. avtorizacija), ki je lahko: <ul style="list-style-type: none"> ○ mobilna telefonska številka za prejem enkratnega gesla, ali ○ Rekono Onepass mobilna aplikacija, aktivirana z Rekono računom in nameščena na pametni mobilni napravi, ali ○ varnostni ključ (oz. druga naprava združljiva s U2F FIDO standardom), ali ○ kvalificirano digitalno potrdilo. - za aktivacijo oz. dvig ravni zaupanja Rekono računa: <ul style="list-style-type: none"> • za dvig ravni zaupanja Rekono računa prek prijave v spletno banko: <ul style="list-style-type: none"> ○ identifikacijski ključ (poslan v dveh delih na e-poštni naslov in mobilno telefonsko številko uporabnika).
Obstoječi avtentikacijski elementi spletne banke	<p>So obstoječi elementi (tj. elementi, ki niso elementi Rekono računa), ki omogočajo varno avtentikacijo uporabnika pri uporabi spletne banke. Ti so:</p> <p>Za uporabo v spletni banki:</p> <ul style="list-style-type: none"> • uporabniško ime za spletno banko,

	<ul style="list-style-type: none"> • kvalificirano digitalno potrdilo (nameščeno na napravi ali na trajnem zaščitenem nosilcu), • stalno vstopno geslo spletne banke, • številka bančne kartice, • PIN koda bančne kartice, • drugi faktor za avtentikacijo: <ul style="list-style-type: none"> ○ mobilna telefonska številka za prejem enkratnega gesla iz spletne banke v SMS sporočilu (SMS žeton), ○ PIN koda za odklep kvalificiranega digitalnega potrdila na trajnem nosilcu, ○ čitalec kartic za ustvarjanje enkratnega gesla z vstavljenjo bančno kartico in PIN kodo kartice. <p>Navedeni avtentikacijski elementi za avtentikacijo v spletni banki so uporabniku na voljo le še do popolnega prehoda na uporabo Rekono računa za avtentikacijo v spletni banki. V času prehoda na uporabo Rekono služijo temu, da se uporabnik v spletno banko prijavi še na obstoječ način, nato pa si iz varnega okolja spletne banke ustvari Rekono račun ustreznih ravni zaupanja.</p>
Aktivacija spletne banke	Je postopek, ki ga izvede uporabnik po vklopu storitve spletne banke imetniku in uporabniku.
Deblokada spletne banke	Je postopek deblokade uporabe spletne banke uporabniku na transakcijskih računih, na katerih je bil uporabniku dostop prek spletne banke na zahtevo zakonitega zastopnika imetnika ali uporabnika predhodno onemogočen (iz varnostnih ali drugih razlogov).
Naprava	Je osebni ali prenosni računalnik, pametni mobilni telefon ali tablični računalnik z operacijskim sistemom Android ali iOS (Android različice 5.0 in višje ali iOS 10.0 in višje), zadostno zmogljivostjo in delovnim pomnilnikom ter posodobljeno različico spletnega brskalnika, ki omogoča uporabo spletne banke.
Uporabniško ime	Je avtentikacijski element, sestavljen iz kombinacije črk in števil. Uporabniško ime uporabnik potrebuje pri prijavi v spletno banko, če izbere način prijave z uporabniškim imenom, vstopnim geslom in SMS žetonom. Uporabniško ime je unikatno.
Kvalificirano digitalno potrdilo (KDP)	Je avtentikacijski element in elektronski identifikacijski instrument imetnika kvalificiranega digitalnega potrdila. Služi avtentikaciji, preverjanju identitete in elektronskemu podpisovanju pri delu s spletno banko. Kvalificirano digitalno potrdilo uporabnik potrebuje pri prijavi v spletno banko, če izbere način prijave s kvalificiranim digitalnim potrdilom in vstopnim geslom (ter SMS žetonom, če kvalificirano digitalno potrdilo ni izdano na varnem nosilcu).
E-poštni naslov	Je edinstveni elektronski naslov uporabnika, ki ga je navedel na Zahtevku za uporabo Poslovne spletne N Banke in služi za prejem elementov aktivacije spletne banke ter obvestil iz spletne banke. E-poštni naslov je tudi osnovni element avtentikacije pri prijavi z Rekono računom. E-poštni naslov za prijavo v Rekono račun in e-poštni naslov za prejem elementa za aktivacijo spletne banke nista nujno enaka.
Mobilna telefonska številka	Je edinstvena mobilna številka uporabnika, ki jo je navedel na Zahtevku za uporabo spletne banke in služi za prejemanje elementov aktivacije spletne banke. Mobilna telefonska številka je tudi eden od možnih elementov dodatne avtentikacije (drugi faktor avtentikacije) pri prijavi z Rekono računom. Mobilna telefonska številka za prijavo v Rekono račun in mobilna telefonska številka za prejem elementa za aktivacijo spletne banke nista nujno enaka. je številka uporabnika, ki jo je imetnik navedel na Zahtevku za uporabo spletne banke SI za pravne osebe in služi za prejemanje drugega dela aktivacijskega elementa.
Vstopno geslo	Je osebno identifikacijsko geslo, sestavljeno iz črk in števil, s katerim se uporabnik identificira pri vstopu v spletno banko oz. v Rekono račun.
PUK koda	Je varnostna koda, sestavljena iz črk in števil, ki uporabniku omogoča ponastavitev dostopa do Rekono računa v primeru pozabljenega vstopnega gesla.
PIN koda (bančne kartice, kvalificiranega digitalnega potrdila, mobilne aplikacije Rekono OnePass)	Je 4 mestno identifikacijsko geslo, sestavljeno iz števil, ki ga uporabnik potrebuje za uporabo svoje N Banka plačilne kartice, oz. je 4 ali več mestno identifikacijsko geslo, sestavljeno iz števil, s katerim imetnik omogoči dostop do kvalificiranega digitalnega potrdila na zaščitenem nosilcu, oz.

	<p>je 4 mestno identifikacijsko geslo, s katerim uporabnik zaščiti dostop do aplikacije Rekono OnePass, nameščene na mobilni napravi.</p> <p>Priporočljivo je, da pri vsakem od navedenih avtentikacijskih elementov oz. naprav, če jih uporablja, uporabnik uporablja različne PIN kode.</p>
Rekono OnePass mobilna aplikacija	<p>Je mobilna aplikacija v okviru Rekono računa in služi kot eden od možnih dodatnih varnostnih elementov (drugi faktor avtentikacije) za avtentikacijo v Rekono računu v okviru EB PO. Rekono OnePass omogoča avtentikacijo prek prejetega potisnega sporočila ali z ustvarjanjem enkratnega časovno omejenega gesla.</p> <p>Dodatno varovanje vstopa v aplikacijo Rekono OnePass je možno s PIN kodo ali z biometričnimi značilnostmi.</p>
Varnostni ključ	<p>Je fizična naprava, ki podpira standard U2F/FIDO in služi kot eden od možnih dodatnih varnostnih elementov (drugi faktor avtentikacije) za avtentikacijo v Rekono računu v okviru uporabe v spletni banki.</p>
Enkratno generirano geslo v SMS sporočilu (SMS žeton)	<p>Je eden od možnih dodatnih varnostnih elementov (drugi faktor avtentikacije) za avtentikacijo v Rekono računu v okviru prijave v spletno banko oz. pri obstoječi prijavi v spletno banko.</p> <p>Uporabnik prejme enkratno časovno omejeno geslo v obliki SMS sporočila na mobilno telefonsko številko, ki jo uporablja v Rekono računu oz. pri obstoječem načinu prijave v spletno banko.</p>
Enkratno generirano geslo v aplikaciji Rekono OnePass	<p>Je enkratno, časovno omejeno geslo, ki ga ustvari aplikacija Rekono OnePass in je eden od možnih dodatnih varnostnih elementov (drugi faktor avtentikacije) za avtentikacijo v Rekono računu v okviru prijave v spletno banko.</p>
Identifikacijski ključ	<p>Je sestavljen iz 16 znakov, kombinacije črk in števil in služi za dvig ravni zaupanja uporabnikovega Rekono računa na ustrezno raven zaupanja, ki zadostuje za uporabnikovo prijavo v spletno banko. Identifikacijski ključ se uporabniku izda ob oddaji vloge in vklopu spletne banke ob osebni identifikaciji v banki in pošlje na e-poštni naslov in mobilno telefonsko številko, ki sta navedena na zahtevku za vklop spletne banke. Identifikacijski ključ poveže uporabnika banke z njegovim Rekono računom.</p> <p>Identifikacijski ključ se uporabniku izda in pošlje ob oddaji vloge in vklopu spletne banke ob osebni identifikaciji v banki. Identifikacijski ključ uporabnik prejme v dveh delih: prvi del, 8 znakov aktivacijskega ključa, prejme na svoj e-poštni naslov, drugi del, 8 znakov, pa na mobilno telefonsko številko. Celotni identifikacijski ključ dolžine 16 znakov, sestavljen iz prvega in drugega dela, uporabnik vpiše pri prijavi z Rekono v spletno banko. Uporabnik bo ob prijavi v spletno banko pozvan, naj uporabi oz. vpiše identifikacijski ključ le, če raven zaupanja v njegov Rekono račun še ne zadostuje za prijavo v spletno banko, v nasprotnem identifikacijskega ključa ni potrebno uporabiti.</p> <p>Uporabnik lahko nov identifikacijski ključ pridobi ob osebni identifikaciji v banki in ga uporabniku izda banka. Uporabi ga lahko, če je ustvarila povsem nov Rekono račun s svojo davčno številko, s katerim se želi prijaviti v spletno banko (prejšnji Rekono račun pa iz različnih razlogov izbrisala).</p> <p>Identifikacijski ključ je veljaven 72 ur od izdaje.</p>
N Banka plačilna kartica	<p>Je poslovna plačilna kartica in je avtentikacijski element, s katerim se uporabnik prijavi v spletno banko; z vpisom številke N Banka plačilne kartice in enkratnim geslom oz. OTP, ki ga na podlagi vpisane PIN kode kartice ustvari OTP čitalec plačilnih kartic.</p>
Enkratno generirano geslo s čitalca kartic	<p>Je avtentikacijski element in je 7- ali 8-mestno število, ki ga ob vpisu PIN kode N Banka plačilne kartice ustvari OTP čitalec plačilnih kartic.</p>
OTP čitalec plačilnih kartic	<p>Je strojna oprema, ki prebere informacije iz čipa na kartici in na podlagi vpisane PIN kode N Banka plačilne kartice ustvari enkratno, časovno omejeno geslo (OTP).</p>
Naročilo	<p>Je zahteva ali povpraševanje za izvedbo bančne storitve, ki jo uporabnik po uspešni avtentikaciji pošlje banki z uporabo spletne banke.</p>
Tarifa	<p>Je vsakokrat veljavna Tarifa nadomestil za storitve banke, ki določa vrsto, višino in način plačevanja nadomestil v zvezi z uporabo spletne banke, in je dostopna na spletnih straneh banke in v vseh poslovalnicah banke</p>
Zahtevek za uporabo	<p>Je Zahtevek za uporabo Poslovne spletne N Banke ali spremembo podatkov Poslovne spletne N Banke.</p>
Zahtevek za deblokado	<p>Je Zahtevek za deblokado uporabe Poslovne spletne N Banke.</p>
Zahtevek za ukinitvev	<p>Je Zahtevek za ukinitvev uporabe Poslovne spletne N Banke.</p>

II. Pridobitev pravice za uporabo spletne banke

3. Člen

Imetnik mora za uporabo spletne banke uporabniku na svoje stroške zagotoviti ustrezne naprave in komunikacijsko opremo z dostopom do interneta oziroma dostopom do mobilnih podatkov. Prav tako si mora za uporabo spletne banke uporabnik ustvariti svoj osebni Rekono račun (neposredno na www.rekono.si ali pa v samem postopku aktivacije oz. prijave v spletno banko).

Minimalne tehnične zahteve so uporabniku dostopne na spletni strani N Banke oziroma v uporabniških navodilih. Uporabnik je dolžan spremljati spremembe minimalnih zahtev in s tem prilagajati svoje naprave in komunikacijsko opremo.

4. Člen

Banka vklopi storitev spletne banke, če so izpolnjeni naslednji pogoji:

- imetnik ima pri banki odprt poslovni transakcijski račun,
- zakoniti zastopnik imetnika odda v celoti pravilno izpolnjen in podpisan Zahtevek za uporabo in drugo dokumentacijo, predpisano v Zahtevku za uporabo, v poslovalnici N Banke ali na sedežu banke,
- uporabnik, ki ga zakoniti zastopnik pooblasti za uporabo spletne banke, je star najmanj 18 let in je poslovno in opravilno sposoben.

S podpisom zahtevka ali potrjenega naročila imetnik potrjuje, da so imetnik in uporabniki seznanjeni z določili teh splošnih pogojev in z določili Tarife ter da jim je znano, da sta navedena akta sestavni del pogodbenega razmerja za uporabo spletne banke.

5. Člen

Vsa nadomestila se poravnajo z neposredno bremenitvijo transakcijskega računa imetnika, s čimer zakoniti zastopnik imetnika s sprejetjem teh splošnih pogojev soglaša.

6. člen

Ob izpolnjenih pogojih iz prejšnjih dveh členov banka izda ustrezne avtentikacijske elemente (identifikacijski ključ za dvig ravni zaupanja v Rekono račun) in jih uporabniku posreduje na elektronski naslov in mobilno telefonsko številko. Uporabnik identifikacijski ključ ob prijavi v spletno banko uporabi za dvig ravni zaupanja v Rekono račun. Z Rekono računom ustrezne ravni zaupanja uporabnik aktivira oz. se lahko prijavi v spletno banko.

Zakoniti zastopnik imetnika potrjuje, da ima uporabnik dostop do e-poštnega naslova in mobilne številke in soglaša z uporabnikovim prejemom avtentikacijskih elementov (identifikacijskega ključa za Rekono račun) za aktivacijo spletne banke. V primeru, da uporabnik ne prejme e-poštnega sporočila ali SMS sporočila z aktivacijskimi elementi (prvi in/ali drugi del identifikacijskega ključa za Rekono račun), mora zakoniti zastopnik imetnika ali uporabnik to nemudoma sporočiti v Kontaktni center banke (na številko 080 22 65), oziroma se mora uporabnik zglasiti v katerikoli poslovalnici banke in zahtevati ponovno pošiljanje identifikacijskega ključa za Rekono račun.

7. Člen

Banka si pridružuje pravico, da Zahtevek za uporabo zavrne brez navedbe razlogov za zavrnitev, o tem pa obvesti imetnika najkasneje v petih delovnih dneh od prejema vloge.

III. Načini dostopa in potrjevanja plačilnih nalogov, naročil in spreminjanje nastavitev

8. Člen

Načini vstopa v spletno banko so opisani v Navodilih za uporabnike spletne banke.

9. člen

Načini potrjevanja plačilnih nalogov, naročil in spreminjanja nastavitev v spletni banki so opisani v Navodilih za uporabnike spletne banke.

IV. Uporaba storitev spletne banke

10. Člen

Spletna banka je način opravljanja bančnih storitev prek spleta oziroma spletne aplikacije, ki uporabnikom glede na dodeljena pooblastila in vrsto in možnost posameznega računa omogoča aktivnosti, kot so: pregled stanja in prometa na transakcijskem računu, poslovnih plačilnih karticah in varčevanjih, vnos oziroma potrjevanje plačil, prenosov sredstev med računi v banki, opravljanje menjalniških poslov, ter izvajanje drugih storitev, ki jih spletna banka omogoča in so opisane v Navodilih za uporabo spletne banke.

Več informacij o spletni banki je objavljenih na spletnih straneh banke in v Navodilih za uporabnike spletne banke. Spletna banka je uporabnikom na voljo v slovenskem in angleškem jeziku.

Izvajanje plačilnih nalogov preko spletne banke se ureja v skladu z Urnikom plačilnega prometa banke in Splošnimi pogoji za opravljanje plačilnih storitev preko transakcijskega računa.

11. Člen

Banka si pridržuje pravico uvajanja novih funkcionalnosti v spletni banki, o čemer bo uporabnike obveščala na spletnih straneh banke, v spletni banki ter v vseh poslovalnicah banke.

Postopek dostopa ter način uporabe spletne banke so opisani v Navodilih za uporabnike spletne banke, ki so dostopna na spletnih straneh banke in v vseh poslovalnicah banke.

V. Pooblastila pri uporabi spletne banke

12. Člen

Zakoniti zastopnik imetnika lahko za uporabo spletne banke pooblasti enega ali več uporabnikov, na enem ali več transakcijskih računih, z enim ali več sklopi pooblastil (vpogled, vnos, podpis), ki se medsebojno dopolnjujejo:

- Vpogled:
 - vpogled v stanje, promet, izpiske transakcijskega računa, poslovno kreditno kartico uporabnika, prejete e-račune, prejete SDD naloge, depozite,
 - možnost dodatnih pooblastil: vpogled v kartični račun (vse poslovne kreditne kartice imetnika, ne glede na transakcijski račun, na katerega so kartice povezane) in/ali vpogled v vsebino paketov množičnih plačil (npr. plače),
 - osebne nastavitve in nastavitve obveščanja.
- Vnos:
 - vnos plačilnega naloga, (prenos) paketa plačilnih nalogov (navadni in množični), vnos (prenos) paketa izdanih SDD nalogov,
 - prijavljanje in odjavljanje na e-račune, menjava valut,
 - oddaja naročil, ki se ne obdelajo avtomatično (povpraševanje za limit, kredit, varnostni SMS, dvig gotovine),
 - možnost dodatnih pooblastil: izdajanje in elektronsko podpisovanje (e-podpis) e-računov,
 - osebne nastavitve.
- Podpis:
 - podpis (potrditev) plačilnega naloga, prejetih e-računov, paketa plačilnih nalogov (navadni in množični), paketa izdanih SDD nalogov,
 - sklenitev depozita (v primeru kolektivnega podpisa, depozit sklence le en podpisnik),
 - preklic prejetega SDD naloga,
 - prijavljanje in odjavljanje na e-račune, menjava valut,
 - oddaja naročil, ki se ne obdelajo avtomatično (povpraševanje za limit, kredit, varnostni SMS, dvig gotovine),
 - možnost dodatnih pooblastil: izdajanje in elektronsko podpisovanje (e-podpis) e-računov,
 - osebne nastavitve, nastavitve potrjevanja plačil, nastavitve obveščanja.

Zakoniti zastopnik lahko uporabniku dodeli tudi pooblastila po meri.

Uporabnik, ki je predhodno uporabljal spletno banko Sberbank Poslovni Splet, je ob prehodu na novo spletno banko samodejno pridobil enak nabor pooblastil, kot jih je imel v spletni banki Sberbank Poslovni Splet, razen pooblastila za vpogled v vsebino paketov množičnih plačil (npr. plače).

V Poslovni spletni N Banki ima uporabnik v sklopu pooblastila za vpogled in izbrane dodatne možnosti pooblastila za vpogled v kartični račun, vpogled v vse poslovne kreditne kartice imetnika, ne glede na transakcijski račun, s katerim so kartice povezane in ne le v poslovne kreditne kartice povezane s transakcijskim računom, na katerega se dano pooblastilo nanaša.

VI. Dolžnosti imetnika in uporabnika

13. Člen

Imetnik se obvezuje, da:

- bo uporabnik pri uporabi spletne banke in ustvarjanju ter uporabi Rekono računa upošteval poleg teh splošnih pogojev, drugih splošnih pogojev in pogodb, ki so kakorkoli povezani ter urejajo opravljanje storitev spletne banke in uporabniških navodil, tudi splošne pogoje za uporabo storitve Rekono in njihove sestavne dele ter veljavno zakonodajo. Uporabnik bo skrbno hranil naprave, preko katerih bo dostopal do spletne banke ter vse možne tipe dostopa in avtentikacijske elemente in jih varoval kot dober gospodar,
- bo preprečil izgubo, krajo ali zlorabo avtentikacijskih elementov ali naprav in jih ne bo širil oziroma posredoval tretjim osebam, pri čemer je odgovoren za vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker so tretje osebe uporabile uporabnikove elemente ali naprave, preko katerih dostopa do spletne banke (uporabniško ime, vstopno geslo, podatek drugega avtentikacijskega faktorja, PIN koda, biometrična značilnost ali identifikacijski ključ) oz. uporabile te elemente za nepooblaščen uporabo Rekono računa;
- bo pri prijavi v Rekono račun v okviru prijave v spletno banko vedno preveril, da je bil preusmerjen oz. se v Rekono račun prijavlja na spletnem naslovu <https://idp.rekono.si>;
- bosta imetnik in uporabnik skrbno izbrala programsko opremo, ki jo uporabnik namešča na svoje naprave v izogib zlonamerni programski opremi (virusi, trojanski konji, ipd), da bo uporabnik imel na svojih napravah nameščen protivirusni program, ter da naprave ne bodo imele omogočenega korenskega dostopa (npr. root, jailbreak, ipd.). Seznam priporočenih protivirusnih programov je objavljen na spletnih straneh banke in na <https://www.cert.si/si/zascita/protivirusna-zascita/>;
- bo Rekono račun in spletno banko ob prejemu aktivacijskih oz. identifikacijskih elementov nemudoma aktiviral; bo naprave, na katerih dostopa do Rekono računa in spletne banke, zavaroval z avtentikacijskimi elementi, ki so drugačni, kot jih uporablja za Rekono račun oz. spletno banko. Pri kreiranju vstopnih gesel oz. PIN kod do naprav, Rekono računa, Rekono OnePass aplikacije pa bo upošteval priporočila za kvalitetno geslo (8 znakov, velike in male črke, številke....) oziroma PIN kodo. Dostop do naprav bo uporabnik zaščiten s funkcijo samodejnega zaklepanja (auto lock) in z uporabo dostopnega gesla (passcode) ter uporabil vse sodobne načine zaščite in tehnologije, objavljene na spletni strani banke ter na <https://www.cert.si/si/zascita/>; uporabnik naprav, na katerih je aktivna spletna banka, ne bo nikoli puščal brez nadzora oziroma se bo vsakokrat ob zaključku uporabe spletne banke odjavil s klikom na gumb odjava;
- na vseh napravah in aplikacijah, ki jih uporablja za avtentikacijo in omogočajo prikaz vsebine SMS in ostalih sporočil oziroma izpis enkratnega gesla na zaklenjenem zaslonu (lock-screen), bo izpis enkratnih gesel na zaklenjenem zaslonu onemogočil. Prav tako bo pri vseh aplikacijah oz. napravah oz. elementih za avtentikacijo (mobilna aplikacija Rekono OnePass, varnostni ključ, kvalificirano digitalno potrdilo v spletnem brskalniku), ki omogočajo dodatno varovanje z geslom ali PIN ali biometrijo, to dodatno varovanje vklopil.
- uporabnik bo, skladno z varnostnimi možnostmi, ki jih omogoča ponudnik e-pošte, poskrbel za največjo možno varnost dostopa do e-poštnih predalov oz. e-poštnih naslovov, ki so prijavljeni v njegov Rekono račun (npr. dostop do poštnega predala bo zaščiten še z drugim avtentikacijskim faktorjem, če je to možno, kot je npr. možno pri ponudniku Gmail).
- bosta zakoniti zastopnik imetnika ali uporabnik takoj obvestila banko o morebitni nepooblaščen uporabi, sumu nepooblaščen uporabe oziroma možnosti nepooblaščen uporabe (npr. če je tretja oseba na kakršenkoli način izvedela ali pridobila avtentikacijski element), kraji ali izgubi naprav, preko katerih uporabnik dostopa do spletne banke;
- bosta zakoniti zastopnik imetnika ali uporabnik v primeru izgube, kraje, zlorabe ali suma na krajo ali zlorabo naprav, preko katerih dostopa do spletne banke ali Rekono računa, to takoj prijavila policiji;
- bosta zakoniti zastopnik imetnika ali uporabnik posredovala banki vse potrebne informacije o okoliščinah, povezanih z izgubo, krajo ali zlorabo naprav preko katerih uporabnik dostopa do spletne banke, da se prepreči nadaljnje nastajanje škode;
- bosta zakoniti zastopnik imetnika ali uporabnik spremljala obvestila o novih različicah in posodobitvah spletne banke;
- bo uporabnik redno nameščal varnostne popravke na operacijski sistem in aplikativne programe in uporabljal varnostne funkcije, ki jih omogočajo naprave (npr. enkripcijo, nameščal samo licenčno programsko opremo, oddaljeno brisanje, »location tracking« in podobne tehnologije) preko katerih dostopa do spletne banke;
- uporabnik na svojih napravah ne bo shranjeval (niti v varni shrambi naprave niti v shrambi brskalnika, sploh pa ne v nezaščitenih datotekah) osebnih informacij oz. informacij o dostopih oz. prijavnih podatkih do spletne banke oz. svojega osebnega Rekono računa; temveč bo avtentikacijske podatke (uporabniško ime, vstopno geslo ipd.) ob vsaki prijavi vpisal v aplikacijo.

- bosta zakoniti zastopnik imetnika ali uporabnik v primeru suma kraje ali zlorabe ter v primeru izgube naprav, preko katerih uporabnik dostopa do spletne banke, ali suma kraje ali zlorabe kateregakoli od avtentikacijskih elementov, ki se uporabljajo za dostop do spletne banke (uporabniško ime, e-poštni naslov, vstopno geslo, mobilna telefonska številka, bančna kartica in PIN koda, ipd.) od banke, preko Kontaktnega centra ali v katerikoli poslovalnici N Banka d.d., v delovnem času Kontaktnega centra oz. bančnih poslovalnic, zahteval takojšnjo blokado storitev spletne banke ter, če je potrebno, blokado tistih avtentikacijskih elementov, ki ji lahko blokira banka. Za blokado drugih avtentikacijskih elementov, ki niso v domeni banke (npr. SIM kartica, dostop do e-poštnega naslova ipd.), poskrbi uporabnik sam;
- bo ob nepooblaščenem uporabi ali ob sumu oz. možnosti nepooblaščenega uporabe, kraji ali izgubi osebnih prijavnih podatkov za dostop do računa storitve Rekono to takoj sporočil banki in pri ponudniku Rekono po elektronski pošti na e-poštni naslov info@rekono.si takoj zahteval blokado Rekono računa ter hkrati obvestil policijo.
- v primeru uporabe kvalificiranega digitalnega potrdila veljajo tudi navodila in/ali splošni pogoji izdajatelja kvalificiranega digitalnega potrdila, objavljena na spletni strani predmetnega izdajatelja. V primeru izgube ali zlorabe kvalificiranega digitalnega potrdila mora imetnik ravnati v skladu z navodili in/ali splošnimi pogoji izdajatelja kvalificiranega digitalnega potrdila;
- bosta zakoniti zastopnik imetnika ali uporabnik ob sumu kraje ali izgube poslovne plačilne kartice ter verjetnosti, da je s PIN kodo kartice seznanjena nepooblaščen oseba, takoj, brez odlašanja, po telefonu obvestil banko ali servisni center. Telefonska številka servisnega centra je zapisana na kartici in objavljena na spletnih straneh banke. Banka ali servisni center bosta blokirala kartico in s tem blokirala tudi dostop s to kartico do spletne banke. Za čas prijave se šteje, ko bančni delavec ali delavec servisnega centra zaključi telefonski pogovor. Uporabnik se obvezuje, da bo banki poleg prej omenjenega podal tudi pisno prijavo o izgubi, poškodbi, kraji ali sumu zlorabe, skladno z veljavnimi splošnimi pogoji banke za poslovne plačilne kartice, objavljenimi na spletnih straneh banke;
- uporabnik bo takoj spremenil vstopna gesla ali PIN kode, po postopku, objavljenem v Navodilih za uporabnike spletne banke, oz. bo takoj spremenil avtentikacijske elemente Rekono računa v primeru, da je zanje izvedela tretja oseba;
- bo uporabnik uporabljal spletno banko v skladu z Navodili za uporabnike spletne banke, določbami teh splošnih pogojev in veljavno zakonodajo;
- uporabnik pri uporabi spletne banke ne bo uporabljal računalniških kod, škodljivih programov ali česar koli, kar bi lahko motilo, onespobilo ali škodovalo uporabi spletne banke, njegovi programski ali strojni opremi ali elektronskem komunikacijskem omrežju; če uporabnik s svojim ravnanjem povzroči škodo, imetnik zanj v celoti odgovarja, tako banki, kot tudi operaterju;
- uporabnik ne bo odgovarjal na e-pošto in SMS sporočila, ki jih ni pričakoval s strani banke;
- uporabnik ne bo klikal na nobeno povezavo, pripeto datoteko ali drugo obliko teksta, prejeta preko e-pošte ali v SMS obliki, v kolikor ni prepričan, da je poslano s strani banke;
- da se bo uporabnik pri uporabi spletne banke povezoval samo z zaupanja vrednimi žičnimi ali brezžičnimi omrežji (vključno z Bluetooth povezavami);
- uporabnik ne bo delil podatkov o spletni banki z drugimi uporabniki;
- bo imetnik zagotavljal sredstva na transakcijskem računu za uporabo spletne banke;
- bosta zakoniti zastopnik imetnika ali uporabnik banko takoj obvestila o vseh nepravilnostih v zvezi z delovanjem spletne banke;
- bo imetnik prevzel vso odgovornost za vse posle, ki jih uporabnik odda prek spletne banke, tudi za morebitno napačno nakazane zneske ali prenose sredstev na napačne račune, če ti sicer obstajajo in so bili prenosi in nakazila izvršeni na zahtevo uporabnika;
- bo zakoniti zastopnik imetnika vsako spremembo uporabnikovega e-poštnega naslova ali mobilne številke sporočil banki, v poslovalnici banke, z uporabo za to namenjenega obrazca oziroma bo mobilno številko v spletni banki določil uporabnik sam,
- bo uporabnik prebral obvestila, ki mu jih banka posreduje ob uporabi spletne banke.

V primeru dvomov v identiteto spletne banke mora uporabnik le-to preveriti prek preverbe kvalificiranega digitalnega potrdila spletnega naslova, ki potrjuje identiteto spletnega naslova.

Imetnik in uporabnik izjavljata, da je uporabnik lastnik e-poštnega naslova in mobilne številke, ki sta navedena na obrazcu ter soglašata s prejemom avtentikacijskih podatkov (identifikacijskega ključa) za dvig ravni zaupanja v Rekono račun in aktivacijo spletne banke na navedeni elektronski naslov in mobilno telefonsko številko uporabnika.

V primeru, da uporabnik ne prejme elektronskih sporočil z identifikacijskimi oziroma aktivacijskimi elementi (prvi in drugi del identifikacijskega ključa), mora to nemudoma sporočiti v Kontaktni center banke (na številko 080 22 65), oziroma se mora uporabnik zglasiti v katerikoli poslovalnici banke in zahtevati ponovno pošiljanje identifikacijskega ključa za svoj Rekono račun.

Imetnik in uporabnik nosi odgovornost za izbiro, uporabo in vzdrževanje naprav, na kateri ima uporabnik uporabljala spletno banko. Imetnik in uporabnik v celoti odgovarja za vso škodo, ki bi nastala njemu ali banki zaradi zlonamerne

kode na uporabnikovih napravah (računalniški virus) ali zaradi druge zlorabe ali nepooblaščne uporabe spletne banke z njegovimi avtentikacijskimi sredstvi.

VII. Dolžnosti banke

14. Člen

Banka se zavezuje, da bo:

- naloge za izvedbo plačilne transakcije, opravljene preko spletne banke in druge bančne storitve, ki jih uporabnik uporablja v spletni banki, izvršila v skladu s Splošnimi pogoji za opravljanje plačilnih storitev preko transakcijskega računa in drugimi splošni pogoji za posamezno storitev ter pogodbami, ki jih ima banka sklenjene z imetnikom ter vsakokrat veljavno zakonodajo,
- svoje obveznosti izvrševala v skladu s pogodbo, temi splošnimi pogoji ter z vsemi drugimi splošnimi pogoji, ki urejajo storitve, ki jih je imetnik sklenil z banko,
- uporabnika v spletni banki oziroma prek sistema obveščanja spletne banke obvestila o morebitni zavrnitvi izvršitve plačilne transakcije,
- spremembe oziroma dopolnitve teh splošnih pogojev, Tarife nadomestil za storitve banke in novosti pri uporabi spletne banke bo banka objavljala na spletnih straneh banke in v spletni banki,
- pri uporabi spletne banke računalniško zapisovala vse postopke, ki jih opravi uporabnik spletne banke (vstop v spletno banko, izstop iz spletne banke ter datum in čas oddaje plačilnih transakcij) in bo skladno z obstoječo zakonodajo skrbela za ustrezno hrambo teh zapisov.

15. Člen

Banka si bo prizadevala, da bo uporaba spletne banke dostopna ves čas. Zaradi vzrokov zunaj njenega nadzora ni izključeno občasno oteženo ali onemogočeno delovanje storitve. Za dostopnost avtentikacijskega sistema Rekono je odgovoren ponudnik storitve Rekono.

Prav tako je lahko zaradi vzdrževanja sistema, ki podpira delovanje spletne banke, delovanje moteno ali prekinjeno, o čemer bo banka uporabnika predhodno obvestila.

16. Člen

Banka ne odgovarja za škodo, ki bi nastala zaradi razlogov, ki so zunaj njenega nadzora in ki jih banka ni mogla preprečiti, odpraviti ali se jim izogniti, vključno z, vendar ne omejeno, izpadi javnega omrežja, kamor še zlasti spadajo vse motnje in prekinitve v telekomunikacijskem prometu, prometu namenjenemu računalniški povezavi, primeri višje sile, stavke, odločitve in dejanja oblastnih organov. Prav tako ne odgovarja za motnje in prekinitve na telekomunikacijskih kanalih ali za napake, nastale pri prenosu podatkov po telekomunikacijskih kanalih ali za onemogočen dostop do spletne banke. Banka ne odgovarja za škodo, ki bi nastala zaradi izpada razpoložljivosti storitve Rekono.

Banka tudi ne odgovarja za težave pri uporabi spletne banke, če na strani uporabnika ni zadoščeno tehničnim pogojem za uporabo spletne banke. Banka ne odgovarja za škodo, ki bi nastala kot posledica napačnega ravnanja ali napačnega posredovanja podatkov s strani zakonitega zastopnika imetnika ali uporabnika spletne banke.

Banka ne odgovarja za morebitno napačno nakazane zneske ali prenose sredstev na napačne račune, če so bili prenos in nakazila izvršeni na zahtevo uporabnika računa.

Odgovornost banke za morebitno škodo je omejena le na navadno škodo. Banka ne odgovarja za škodo iz naslova izgubljenega dobička ali za nepremoženjsko škodo.

Banka v nobenem primeru ne odgovarja za zlorabe, ki bi bile posledica predaje ali posojanja obstoječih avtentikacijskih elementov, kvalificiranih digitalnih potrdil ali Rekono uporabniškega računa drugim osebam.

VIII. Odgovornost imetnika

17. Člen

Banka in imetnik odgovarjata za neodobrene, nepravilne oziroma neizvršene plačilne transakcije skladno s Splošnimi pogoji za opravljanje plačilnih storitev preko transakcijskega računa, predpisi, ki urejajo plačilne storitve in splošnimi pravili obligacijskega prava.

Imetnik krije celoten znesek škode zaradi neodobrene plačilne transakcije in pripadajočih nadomestil ter obresti, če je izvršitev neodobrene plačilne transakcije:

- posledica imetnikove ali uporabnikove prevare ali če uporabnik ni izpolnil svojih obveznosti v zvezi z ukrepi za zaščito skladno s temi splošnimi pogoji,
- posledica kraje ali izgube varnostnih elementov in naprav,
- posledica zlorabe spletne banke imetnika,
- imetnik izrecno ne želi, da Banka izvede blokado spletne banke v skladu s temi splošnimi pogoji,
- kršitve teh splošnih pogojev.

Ne glede na določbe tega člena, banka imetniku povrne celotno izgubo zneska neodobrene plačilne transakcije in pripadajočih nadomestil ter obresti, ki nastanejo po tem, ko je imetnik ali uporabnik banko obvestil o zlorabi spletne banke, izgubi ali kraji varnostnih elementov in naprav, skladno s temi splošnimi pogoji, in po tem ko je banka lahko izvedla blokado skladno s temi splošnimi pogoji. Banka se razbremeni odgovornosti po tem odstavku, v kolikor je škoda posledica imetnikovega ali uporabnikovega ravnanja.

18. Člen

Če imetnik ali uporabnik sumi, da je bil avtentikacijski element prestrežen, zlorabljen, ukraden, zlorabljen ali je bila z njim seznanjena tretja oseba, ali mu je bila ukradena naprava, ki jo uporablja za dostop do spletne banke, mora:

- obvestiti banko na način in v skladu s temi splošnimi pogoji,
- uporabnik takoj zamenjati avtentikacijske elemente, oz. v kolikor gre za avtentikacijske elemente Rekono računa, pa le-teh uporabnik iz različnih razlogov ne more zamenjati, mora pri Rekono (info@rekono.si) nemudoma zahtevati ukinitvev Rekono računa,
- imetnik takoj vložiti zahtevek za izdajo novih avtentikacijskih oz. identifikacijskih elementov v katerikoli poslovalnici banke v okviru urnika poslovanja,
- imetnik ali uporabnik zahtevati blokado spletne banke uporabniku, če obstaja sum zlorabe, v Kontaktnem centru banke ali v katerikoli poslovalnici banke v okviru urnika poslovanja, ki je objavljen v spletni banki ter na spletni strani banke,

Uporabnik vložiti zahtevek za izdajo novih avtentikacijskih oziroma identifikacijskih elementov (identifikacijski ključ za dvig ravni zaupanja v Rekono računa ob prijavi v spletno banko) v poslovalnici N Banke. Uporabnik zahteva ponastavitev dostopa do Rekono računa, ki ga uporablja za dostop do spletne banke, s pomočjo prejete nove PUK kode (na svoj e-poštni naslov oziroma mobilno telefonsko številko) prek Kontaktnega centra banke oziroma zahteva blokado spletne banke v Kontaktnem centru banke ali v poslovalnici N Banke.

Zakoniti zastopnik imetnika odda Zahtevek za deblokado v poslovalnici banke.

IX. Začasna blokada uporabe spletne banke

19. Člen

Banka začasno blokira dostop do spletne banke (blokada je avtomatska le v primeru iz prve alineje, sicer pa na zahtevo), kadar:

- uporabnik doseže določeno število napačnih prijav z avtentikacijskimi elementi (skladno z Navodili za uporabnike spletne banke),
- zakoniti zastopnik imetnika ali uporabnik prijavi izgubo, krajo ali nepooblaščen dostop do naprave, preko katere dostopa do spletne banke in/ali do enega izmed možnih dostopov do spletne banke (začasno blokira spletno banko),
- zakoniti zastopnik imetnika želi uporabniku blokirati dostop do posameznega ali vseh transakcijskih računov imetnika,
- obstaja sum o možnosti nepooblaščenega dostopa do spletne banke.

Zakoniti zastopnik imetnika lahko začasno blokira spletno banko posameznemu uporabniku za posamezen račun, ali pa uporabnik sebi začasno blokira spletno banko na vseh računih, na katerih je pooblaščen:

- s klicem v Kontaktni center v okviru delovnega časa Kontaktnega centra (blokada takoj), ali
- s sporočilom prek Komunikacijskega centra v spletni banki:
 - sporočilo prejeto do 17:00, blokada isti dan v okviru delovnega časa Kontaktnega centra,
 - sporočilo prejeto po 17:00, blokada isti dan, oziroma naslednji delovni dan do 9:00 ure.

Banka o začasni blokadi spletne banke iz razlogov, navedenih v prvi alineji prvega odstavka tega člena, uporabnika seznaniti na vstopnem zaslonu spletne banke takoj ob naslednjem poskusu vstopa v spletno banko.

V primeru razlogov, navedenih v drugi, tretji in četrti alineji prvega odstavka tega člena, uporabnik po vstopu v spletno banko nima več dostopa do računa, do katerega je dostop uporabniku blokirano.

Odprava začasne blokade spletne banke se izvede, ko so odpravljeni vsi razlogi začasne ustavitve uporabe in ko zakoniti zastopnik imetnika odda Zahtevek za deblokado.

Uporabnik, kateremu je banka začasno blokirala dostop do spletne banke zaradi preseženega števila napačnih poskusov prijav v spletno banko, si lahko deblokira dostop do spletne banke tako, da pokliče v Kontaktni center banke in zahteva ponastavitev števca napačnih poskusov dostopa do spletne banke.

Plačilni nalogi, ki se nahajajo v čakalni vrsti v trenutku blokade spletne banke, se izvedejo ne glede na začasno onemogočeno uporabo spletne banke, če so izpolnjeni pogoji za njihovo izvršitev.

Če je uporabnik pozabil vstopno geslo Rekono računa, mu banka pošlje ponastavitveno povezavo za dostop do Rekono računa (na podlagi klica ali poslanega e-poštnega sporočila v Kontaktni center banke). Če je uporabnik izbrisal Rekono račun in ustvaril novega, se uporabnik zgledi v poslovalnici, kjer mu na podlagi zahtevka banka izda nov identifikacijski ključ za Rekono račun.

X. Obveščanje uporabnikov

20. Člen

Uporabnik se lahko v spletni banki naroči na prejemanje brezplačnih e-poštnih in/ali SMS obvestil glede na kriterije, ki jih določi v spletni banki, na svoj e-poštni naslov ali mobilno številko.

Zakoniti zastopnik imetnika in uporabnik sta odgovorna za navedbo pravih kontaktnih podatkov. Banka se zavezuje, da bo uporabniku posredovala dogovorjena e-poštna in/ali SMS obvestila, razen v primeru višje sile ali razlogov, ki so na strani podjetja, ki izvaja distribucijo podatkov. Višja sila pomeni vsako nepredvidljivo in izjemno okoliščino ali dogodek, ki je zunaj nadzora banke in je/ga ni mogoče pripisati njeni napaki ali malomarnosti.

XI. Prenehanje uporabe spletne banke

21. Člen

Imetnik lahko kadarkoli preneha uporabljati storitev, ki jo opredeljujejo ti splošni pogoji, kar stori tako, da pisno ukine uporabo spletne banke. To stori z obrazcem Zahtevek za ukinitvev uporabe Poslovne spletne N Banke, ki ga odda v poslovalnici banke. Banka ukine spletno banko najpozneje v petih (5) delovnih dneh po prejemu imetnikovega Zahtevka za ukinitvev spletne banke. Oddaja zahtevka za ukinitvev spletne banke ne pomeni takojšnje blokade uporabe spletne banke. V primeru, če želi imetnik takoj blokirati uporabo spletne banke, preden je storitev dokončno ukinjena, mora oddati zahtevo za blokado na druge načine, ki so opisani v teh splošnih pogojih.

Imetnik lahko z Zahtevkom za ukinitvev:

- ukine uporabnika spletne banke pri imetniku (uporabniku se ukine dostop do vseh transakcijskih računov imetnika),
- ukine uporabniku spletne banke pri imetniku dostop do posameznega transakcijskega računa imetnika,
- ukine spletno banko imetniku in vsem uporabnikom, pooblaščenim za uporabo spletne banke pri imetniku.

22. Člen

V primeru, da uporabnik plačilnih transakcij v čakalni vrsti ni preklical, se te izvedejo v skladu z Urnikom plačilnega prometa banke.

Vse obveznosti imetnika, nastale do dneva ukinitvev uporabe spletne banke, se ne glede na prenehanje uporabe spletne banke, izvršijo v skladu z določili teh splošnih pogojev.

Odpoved oz. ukinitvev uporabe spletne banke pomeni, da banka uporabniku zapre oz. izklopi servis spletne banke in prijava vanjo z aktivnim Rekono računom ni več možna. Ukinitvev uporabe spletne banke posameznemu uporabniku ne pomeni tudi ukinitvev servisa spletne banke imetniku, niti Rekono uporabniškega računa.

23. Člen

Banka lahko uporabniku ukine spletno banko brez odpovednega roka v naslednjih primerih:

- če zakoniti zastopnik imetnika odda Zahtevek za ukinitvev,
- če imetnik banki ali banka imetniku odpove Okvirno pogodbo o odprtju in vodenju transakcijskega računa, na katerega je vezana uporaba spletne banke,
- če uporabnik krši te splošne pogoje ali katerokoli drugo pogodbo, sklenjeno z banko, pa niti po opozorilu banke ne preneha s kršitvijo,
- če je ob sklenitvi pogodbe navedel neresnične podatke,

- če imetnik banki nemudoma ne sporoči vsako spremembo podatkov in drugih pogojev, ki so vplivali na odločitev o odobritvi uporabe spletne banke,
- če tako zahteva zakonodaja ali pristojni organ.

Vse pravice iz naslova uporabe spletne banke skladno s temi splošnimi pogoji prenehajo z ukinitvijo spletne banke. Vse obveznosti iz naslova uporabe spletne banke skladno s temi splošnimi pogoji prenehajo po tem, ko imetnik poravna vsa nadomestila in stroške.

XII. Pomoč uporabnikom

24. Člen

Pomoč za nemoteno in pravilno uporabo spletne banke zagotavlja Kontaktni center banke na brezplačni telefonski številki 080 22 65, ki je uporabniku dosegljiv v okviru urnika poslovanja, ki je objavljen na spletnih straneh banke.

XIII. Nadomestila in stroški

25. Člen

Banka imetniku za storitve, povezane s spletno banko in opravljanje plačilnih transakcij ter drugih storitev zaračunava nadomestila in stroške v skladu z vsakokrat veljavno Tarifo banke, ne glede na to ali je vlogo/zahtevek/spremembo podal oz. izvedel imetnik ali uporabnik, če banka to omogoča. Banka svoje terjatve poravna z bremenitvijo transakcijskega računa imetnika, o čemer ga obvesti z izpiskom in s čimer zakoniti zastopnik imetnika soglaša s sprejetjem teh splošnih pogojev. Tarifa je na voljo v vsaki poslovalnici banke in na spletnih straneh banke.

XIV. Reklamacije, reševanje sporov

26. Člen

Reklamacije

Uporabnik mora podati reklamacijo v pisni obliki, ki jo lahko vloži osebno v vsaki poslovalnici banke ali jo pošlje na naslov banke ali jo posreduje preko spletne banke.

27. Člen

Mirno reševanje sporov

Morebitne spore ali pritožbe v zvezi z opravljanjem storitev v skladu s temi splošnimi pogoji bosta uporabnik in banka reševala sporazumno v skladu s Pravilnikom o pritožbenem postopku in zunajsodnem reševanju sporov, ki je uporabniku na vpogled na vidnem in dostopnem mestu v vsakem prostoru, kjer banka posluje s strankami in na spletni strani banke.

Pritožbo v zvezi z opravljeno storitvijo banke lahko uporabnik posreduje banki na prvi stopnji: pisno – osebno v poslovni enoti, po pošti na naslov sedeža banke, preko spletne banke, po elektronski pošti ali preko obrazca na naši spletni strani ter ustno – osebno v poslovni enoti ali po telefonu ter na drugi stopnji (pritožba na Komisijo za pritožbe) le pisno – po pošti, na naslov sedeža banke.

Banka mora uporabniku na pritožbo odgovoriti: na prvi stopnji v roku 8 dni in na drugi stopnji v roku 15 dni oz. ga v tem roku obvestiti, da je pritožba v obravnavanju in o predvidenem času rešitve zadeve, kadar gre za vsebinsko zahtevnejše primere ali kadar odgovora v predpisanem roku ni mogoče predložiti. Odločitev o pritožbi pošlje banka uporabniku v pisni obliki na naslov, ki ga je uporabnik navedel v pritožbi.

Za reševanje vseh morebitnih sporov, ki bi nastali na podlagi teh splošnih pogojev in jih uporabnik ter banka ne bi uspela rešiti sporazumno, je pristojno sodišče v po sedežu banke. Ne glede na določbo prvega odstavka tega člena, lahko banka po svoji izbiri sproži ustrezne sodne postopke tudi pred katerikoli drugim krajevno pristojnim sodiščem.

XV. Varovanje zaupnih podatkov

28. Člen

Banka obdeluje, hrani, varuje vaše osebne podatke skladno z vsakokrat veljavnim zakonom, ki ureja varstvo osebnih podatkov, Splošno uredbo EU o varstvu podatkov (Uredba (EU) 2016/679 – GDPR) in svojimi internimi akti, za izvajanje medsebojnega pogodbenega odnosa z vami ter skladno z vašo privolitvijo, če je bila ta podana, za obdelavo osebnih podatkov za namene trženja. Banka bo z osebnimi podatki pogodbenih strank ravnala tako, da ne bo prišlo do morebitnih neupravičenih posredovanj podatkov nepooblaščenim osebam, na način, kot je to

določeno v vsakokrat veljavnih Splošnih informacijah o varstvu osebnih podatkov, dostopnih tudi na spletnih straneh banke: <https://www.nbanka.si/pripomocki/poti-do-banke/varstvo-osebnih-podatkov/splosne-informacije-o-varstvu-osebnih-podatkov>, ki so sestavni del teh splošnih pogojev poslovanja. Z vsebino navedenega dokumenta in možnostjo pridobitve le tega v tiskani obliki, banka seznaní imetnika ob oddaji vloge, imetnik pa o tem seznaní uporabnika.

Informacije in podatki, ki se nanašajo na opravljanje storitev na podlagi teh splošnih pogojev so zaupne narave. Banka daje te podatke le imetniku in skladno z zakonom pristojnim organom na njihovo pisno zahtevo. Dolžnost varovanja zaupnih podatkov ne velja, če banka te podatke posreduje tožilstvu ali policiji, z namenom, da naznani razloge za sum, da je bilo storjeno kaznivo dejanje. Ponudniki plačilnih storitev in udeleženci plačilnih sistemov lahko zbirajo, obdelujejo in izmenjujejo zaupne podatke, vključno z osebnimi podatki o uporabnikih z namenom preprečevanja, preiskovanja ali odkrivanja goljufij ali prevar v zvezi s plačilnimi storitvami v skladu z ZPlaSSIED.

Banka kot upravljavec osebnih podatkov posreduje osebne podatke, s katerimi razpolaga na podlagi pogodbenega razmerja z uporabnikom, za namen poenotenja bančnih operacij, nadzora in izvajanja medsebojnega pogodbenega odnosa v okviru bančne skupine, drugim uporabnikom osebnih podatkov in pogodbenim obdelovalcem, tudi izven ozemlja Republike Slovenije, ki s tem pridobijo pravico obdelovanja posredovanih osebnih podatkov.

Podatki o poslovanju s spletno banko so poslovna skrivnost in se smejo sporočiti tretjim osebam le v skladu z veljavnimi predpisi.

Banka komunicira z zakonitim zastopnikom imetnika in uporabnikom preko komunikacijskih medijev (e-poštni naslov, mobilna številka), ki jih je zakoniti zastopnik imetnika posredoval banki za namen izvajanja storitve spletne banke. Z uporabnikom komunicira banka tudi preko spletne banke, z imetnikom pa lahko tudi po pošti.

Zakoniti zastopnik imetnika in uporabnik sta seznanjena, da banka lahko opravi poizvedbo o njegovih osebnih in drugih podatkih, med drugim zlasti o prebivališču, EMŠO in davčni številki pri upravljavcih zbirk podatkov, če jih banka ne bi imela oziroma jih ni banki osebno posredoval, pa so ti podatki potrebni za doseg namena teh splošnih pogojev. Banka bo osebne in druge podatke zbrisala iz svojih zbirk podatkov, ko bo dosežen namen pogodbe oziroma ko bo potekel rok, ki predpisuje dobo hranjenja teh podatkov.

Imetnik je seznanjen, da banka lahko opravi poizvedbo o njegovem premoženju in nepremičnem premoženju, terjativah, deležih, delnicah in drugih vrednostnih papirjih, številkah računov pri bankah in plačilnih institucijah ter drugem njegovem premoženju in drugih podatkih pri drugih upravljavcih zbirk podatkov, če jih banka ne bi imela oziroma jih ni banki posredoval, pa so ti podatki potrebni za doseg namena teh splošnih pogojev. Banka bo podatke zbrisala iz svojih zbirk podatkov, ko bo dosežen namen pogodbe oziroma ko bo potekel rok, ki predpisuje dobo hranjenja teh podatkov.

XVI. Končne določbe

29. Člen

V primeru, da bo Banka spremenila te splošne pogoje, bo o tem imetnika in uporabnika seznanila ali prek spletne banke ali na Spletni strani banke ob uveljavitvi spremenjenih splošnih pogojev. Če imetnik ne soglašá s spremembami splošnih pogojev, lahko brez odpovednega roka in plačila nadomestil odstopi od uporabe storitve/pogodbe (ukinitev storitve spletne banke), sklenjene na podlagi teh splošnih pogojev. Odstop od pogodbe mora imetnik podati najkasneje v 15 dneh od začetka veljave sprememb. Če imetnik v tem roku Banki ne sporoči, da se s spremembami ne strinja, se šteje, da s spremembami soglašá.

V primeru, da imetnik zavrne predlagane spremembe najkasneje v 15 dneh od začetka veljave sprememb in pri tem ne odpove pogodbi, se šteje, da je Banka odpovedala pogodbo s 15 dnevni odpovedni rokom, ki teče od dneva, ko imetnik zavrne predlagane spremembe.

Vsakokrat veljavni splošni pogoji bodo objavljeni na spletnih straneh banke in na voljo v vseh poslovalnicah banke.

Za opravljanje storitev v skladu s temi splošnimi pogoji in za tolmačenje le-teh se uporablja pravo Republike Slovenije.

Ti splošni pogoji so sestavni del Zahtevka za uporabo spletne banke, ki velja kot pogodba.

Če uporabnik zazna, da je pri opravljanju storitev na podlagi teh splošnih pogojev prišlo do kršitve, ki predstavlja prekršek po ZPlaSSIED, ima pravico vložiti pisni predlog za uvedbo postopka o prekršku. Predlog se vloží pri Banki Slovenije, ki je pristojna za odločanje o tovrstnih prekrških in nadzor nad poslovanjem banke.

Splošni pogoji veljajo od 22.04.2022 in pod pogojem, da se bo takrat pričel prehod na uporabo novih avtentikacijskih načinov Rekono v spletni banki. V nasprotnem primeru se začetek veljavnosti teh splošnih pogojev

prestavi do dneva pričetka dejanskega prehoda na avtentikacijske načine Rekono, v tem vmesnem času pa ostanejo v veljavi prejšnji splošni pogoji.

Veljajo od 22.04.2022