SPLOŠNI POGOJI POSLOVANJA ZA UPORABNIKE DIGITALNIH BANČNIH POTI ZA FIZIČNE OSEBE

I. UVODNE DOLOČBE

1. člen

Izdajatelj splošnih pogojev poslovanja za uporabo Digitalnih bančnih poti (v nadaljevanju besedila: DBP) je N Banka d.d., (v nadaljevanju besedila: banka), Dunajska cesta 128a, 1000 Ljubljana. N Banka d.d. ima dovoljenje Banke Slovenije za opravljanje plačilnih storitev.

S temi splošnimi pogoji so določene pravice, obveznosti in pogoji za uporabo DBP za fizične osebe.

Za vse, kar ni posebej urejeno s temi splošnimi pogoji, se uporabljajo Splošni pogoji za opravljanje plačilnih storitev preko transakcijskega računa za potrošnike 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 preko transakcijskega računa za potrošnike 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 Zahtevka za uporabo Spletne N Banke ali Zahtevka za uporabo Mobilne N Banke (v nadaljevanju: Zahtevek za uporabo DBP) za fizične osebe sklenjenega med banko in imetnikom transakcijskega ali kartičnega računa oziroma zakonitim zastopnikom in imajo značaj pogodbe. S podpisom uporabnika na Zahtevku za uporabo DBP imajo ti splošni pogoji značaj pogodbe tudi v razmerju med banko in uporabnikom.

Sestavni del teh splošnih pogojev so:
- Urnik izvrševanja plačilnih transakcij pri banki,
- Splošni pogoji za opravljanje plačilnih storitev preko transakcijskega računa za potrošnike,
- Tarifa nadomestil za storitve banke
- Navodila za uporabnike Spletne N Banke in Navodila za uporabnike Mobilne N Banke (oboja navodila skupaj v nadaljevanju: uporabniška navodila).

II. OPREDELITEV POJMOV

2. člen

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

Digitalne bančne poti (v nadaljevanju: DBP)	so bančne poti, ki uporabnikom Digitalnih bančnih poti z različnimi programskimi in komunikacijskimi aplikacijami omogočajo opravljanje bančnih in drugih finančnih storitev. Sem sodita Spletna N banka in Mobilna N Banka.
Spletna N Banka (v nadaljevanju: spletna banka)	je elektronski način poslovanja in opravljanja plačilnih transakcij in drugih bančnih storitev preko spletne aplikacije.
Mobilna N Banka (v nadaljevanju: mobilna banka)	je elektronski način poslovanja in opravljanja plačilnih transakcij in drugih bančnih storitev preko mobilne aplikacije.
Imetnik računa	je imetnik transakcijskega, varčevalnega ali kartičnega računa v N Banka d.d.
Pooblaščenec	je polnoletna fizična oseba, ki je poslovno sposobna in ki jo imetnik računa pooblasti za uporabo DBP.
Zakoniti zastopnik	je zakoniti zastopnik ali skrbnik, ki na podlagi zakona ali pooblastila, danega z odločbo pristojnega organa, zastopa imetnika računa, ki je omejeno poslovno sposoben ali ni poslovno sposoben.
Uporabnik DBP (v nadaljevanju: uporabnik)	je fizična oseba, ki je imetnik računa oz. pooblaščenec ali zakoniti zastopnik, ki mu je banka odobrila uporabo spletne banke in/ali mobilne banke.
Pristopnina	je znesek, ki ga uporabnik plača za vklop spletne in/ali mobilne banke. Ob plačilu pristopnine se šteje, da je uporabnik izrazil voljo po uporabi spletne in/ali mobilne banke.
Naročnina	je mesečni znesek, ki ga uporabnik plačuje za najem spletne ali mobilne banke, ki uporabniku omogoča opravljanje plačilnih transakcij in drugih bančnih storitev razpoložljivih v spletni ali mobilni banki. Pogoj za zaračunavanje naročnine je plačilo pristopnine, neodvisno ali se spletna oz. mobilna banka tudi dejansko uporablja.
Vklop in aktivacija DBP	je tehnično stanje, ki sledi plačilu pristopnine in s katerim banka uporabniku vklopi storitev spletne in/ali mobilne banke. Aktivacijo spletne oz. mobilne banke izvede uporabnik sam, skladno z navodili za uporabo spletne oz. mobilne banke.

Mobilna aplikacija Mobilna N Banka	je mobilna aplikacija, ki si jo uporabnik mobilne banke naloži na svojo mobilno napravo v spletnih trgovinah Apple Store (za naprave z operacijskim sistemom iOS) oziroma Google Play ali Huawei App Gallery (za naprave z operacijskim sistemom Android).
Naprava	je osebni računalnik oz. pametni mobilni telefon ali tablični računalnik z ustreznim spletnim brskalnikom oziroma mobilnim operacijskim sistemom Android oz. iOS, ki omogoča uporabo spletne oz. namestitev mobilne aplikacije in aktivacijo DBP. Priporočene oz. še podprte različice mobilnih operacijskih sistemov oz. brskalnikov so navedene v navodilih za uporabo spletne oz. mobilne banke.
Rekono storitev	Rekono je družina rešitev in storitev za elektronsko identifikacijo, elektronske podpise in druge storitve zaupanja, ki posameznikom, podjetjem, bankam, organizacijam in vladnim agencijam 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. 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. Uporabnik prične Rekono storitev uporabljati tako, da si ustvari Rekono račun.
Rekono e-identiteta	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 ali mobilni banki pridobi z identifikacijo v banki ali z drugimi načini, ki so možni v okviru storitve Rekono. V nadaljevanju teh splošnih pogojev za Rekono e-identiteto ustrezne ravni zaupanja uporabljamo poenostavljen izraz Rekono račun ustrezne ravni zaupanja.
Rekono račun	uporabnik ustvari Rekono uporabniški račun (v nadaljevanju: Rekono račun), ki je nosilec uporabnikove Rekono e-identitete določene ravni zaupanja. 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 ali mobilne banke. Rekono račun ustrezne ravni zaupanja se v postopku aktivacije spletne ali mobilne banke poveže s fizično osebo. Z Rekono računom ustrezne ravni zaupanja uporabnik tako vstopa v spletno oziroma mobilno banko, izvaja avtorizacijo aktivnosti in podpisuje dokumente, kjer je to zahtevano. Uporabnik Rekono račun za uporabo z digitalnimi bančnimi potmi uporablja skladno s splošnimi pogoji za uporabo Rekono na https://www.rekono.si/sl/kako-deluje/splosni-pogoji/ in s temi splošnimi pogoji.
Avtentikacijski elementi Rekono	so elementi, ki omogočajo varno avtentikacijo uporabnika pri uporabi Rekono računa v spletni ali mobilni banki. Med te spadajo: - za uporabo v **spletni ali mobilni banki** ob uporabi avtentikacije z Rekono računom: • 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: o mobilna telefonska številka za prejem enkratnega gesla, ali o Rekono Onepass mobilna aplikacija, aktivirana z Rekono računom in nameščena na pametni mobilni napravi, ali o varnostni ključ (oz. druga naprava združljiva s U2F FIDO standardom), ali o kvalificirano digitalno potrdilo.

	- za aktivacijo oz. dvig ravni zaupanja Rekono računa: • za dvig ravni zaupanja Rekono računa prek prijave v spletno ali mobilno banke: ○ identifikacijski ključ (poslan v dveh delih na e-poštni naslov in mobilno telefonsko številko uporabnika).
Obstoječi avtentikacijski elementi spletne in mobilne banke	so obstoječi elementi (tj. elementi, ki niso elementi Rekono računa), ki omogočajo varno avtentikacijo uporabnika pri uporabi spletne ali mobilne banke. Med te spadajo. Za uporabo v **spletni banki:** • uporabniško ime za spletno banko, • 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: ○ 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 vstavljeno bančno kartico in PIN kodo kartice. 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 si uporabnik uspešno ustvari Rekono račun ustrezne ravni zaupanja. Za uporabo v **mobilni banki**: • uporabniško ime za mobilno banko, • stalno vstopno geslo (ali PIN) oziroma biometrična značilnost // s samodejnim generiranjem časovno omejene enkratne kode v ozadju. Navedeni privzeti avtentikacijski elementi za avtentikacijo v mobilni banki so uporabniku na voljo tudi po prehodu na uporabo Rekono računa za avtentikacijo v mobilni banki.
Uporabniško ime	je avtentikacijski element, sestavljen iz kombinacije črk in številk, ki se uporablja ob prijavi v spletno oziroma mobilno banko. Različna uporabnika ne moreta imeti enakega uporabniškega imena.
Kvalificirano digitalno potrdilo	je kvalificirano potrdilo kot je urejeno v Zakonu o elektronski identifikaciji in storitvah zaupanja (v nadaljevanju: ZEISZ) oz. pravnem aktu, ki bo nasledil ZEISZ in predstavlja avtentikacijski element, ki se uporablja ob prijavi v spletno banko.
E-poštni naslov	je edinstveni elektronski naslov uporabnika, ki ga je navedel na Zahtevku za uporabo spletne ali mobilne banke in služi za prejem elementov aktivacije spletne ali mobilne banke ter obvestil iz spletne ali mobilne 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 ali mobilne banke nista nujno enaka.
GSM/ mobilna številka	je **edinstvena** mobilna številka uporabnika, ki jo je navedel na Zahtevku za uporabo spletne ali mobilne banke in služi za prejemanje elementov aktivacije spletne ali mobilne banke ter obvestil iz spletne banke. Mobilna telefonska številka je tudi eden od možnih elementov dodatne avtentikacije (drugi faktor avtentikacije) pri prijavi z Rekono računom oz. obstoječim načinom prijave v spletno banko. Mobilna telefonska številka za prijavo v Rekono račun in mobilna telefonska številka za prejem elementa za aktivacijo spletne ali mobilne banke nista nujno enaka.

Plačilna kartica	je kartica, ki služi avtentikaciji uporabnika in je hkrati varnostni instrument, s katerim se uporabnik identificira in avtenticira ob prijavi v spletno banko. Banka za ta namen uporablja debetne Mastercard kartice transakcijskega računa in Ide@l Mastercard kartice za imetnike kartičnega računa.
Vstopno geslo	je osebno identifikacijsko geslo, sestavljeno iz črk in številk, s katerim se uporabnik identificira pri vstopu v spletno ali mobilno banko oz. v Rekono račun.
PUK koda Rekono	je varnostna koda, sestavljena iz črk in številk, ki uporabniku omogoča ponastavitev dostopa do Rekono računa v primeru pozabljenega vstopnega gesla.
PIN koda (bančne kartice, mobilne banke, kvalificiranega digitalnega potrdila PIN koda KDP, PIN koda mobilne aplikacije Rekono OnePass, mobilne naprave)	je 4 mestno identifikacijsko geslo, sestavljeno iz številk, s katerim se uporabnik prijavi v mobilno banko, oz. je 4 mestno identifikacijsko geslo, sestavljeno iz številk, ki ga uporabnik potrebuje za uporabo svoje plačilne kartice, oz. je 4 ali več mestno identifikacijsko geslo, sestavljeno iz številk, s katerim imetnik omogoči dostop do kvalificiranega digitalnega potrdila na zaščitenem nosilcu, oz. je 4 mestno identifikacijsko geslo, s katerim uporabnik zaščiti dostop do aplikacije Rekono OnePass, nameščene na mobilni napravi, oz. je 4 ali več mestno identifikacijsko geslo, s katerim uporabnik zaščiti napravo, na kateri dostopa do spletne ali mobilne banke. Priporočljivo je, da pri vsakem od navedenih avtentikacijskih elementov oz. naprav, če jih uporablja, uporabnik uporablja različne PIN kode.
Avtentikacija z biometričnimi značilnostmi	je način avtentikacije uporabnika, ki temelji na osebni biometrični značilnosti uporabnika - prstnem odtisu ali prepoznavanjem obraza. Uporaba avtentikacije z biometričnimi značilnostmi je možna v mobilni banki in v mobilni aplikaciji Rekono OnePass.
Rekono OnePass mobilna aplikacija	je mobilna aplikacija v okviru Rekono računa in v naboru storitev banke služi kot eden od možnih dodatnih varnostnih elementov (drugi faktor avtentikacije) za avtentikacijo v Rekono računu v okviru digitalnih bančnih poti. Rekono OnePass omogoča avtentikacijo prek prejetega potisnega sporočila ali z ustvarjanjem enkratnega časovno omejenega gesla. Dodatno varovanje vstopa v aplikacijo Rekono OnePass je možno s PIN kodo ali z biometričnimi značilnostmi.
Varnostni ključ	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 ali mobilni banki.
Enkratno generirano geslo v SMS sporočilu (SMS žeton)	eden od možnih dodatnih varnostnih elementov (drugi faktor avtentikacije) za avtentikacijo v Rekono računu v okviru prijave v spletno ali mobilno banko oz. pri obstoječi prijavi v spletno banko. 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.
Enkratno generirano geslo v aplikaciji Rekono OnePass	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 ali mobilno banko.
Enkratno generirano geslo s čitalca kartic	je 8-mestno število, ki ga ustvarja čitalec plačilnih kartic (»OTP čitalec«) in služi kot avtentikacijski element pri prijavi v spletno banko.
Enkratno generirano geslo v mŽetonu	je 8-mestno število, ki ga ustvari generator mŽeton v mobilni banki in služi kot avtentikacijski element za potrditev spletnega nakupu s plačilno kartico.
Čitalec plačilnih kartic (OTP čitalec)	je strojna oprema, ki ob vnosu plačilne kartice in pravilne PIN kode prebere informacije iz čipa na kartici in generira enkratno geslo.
Tarifa	je vsakokrat veljavna Tarifa nadomestil za storitve banke, ki določa vrsto, višino in način plačevanja nadomestil v zvezi z uporabo DBP, dostopna na spletni strani https://www.nbanka.si/pripomocki/pogoji-poslovanja/cenik-storitev in v vseh poslovalnicah, kjer posluje N Banka.
Identifikacijski ključ	je sestavljen iz 16 znakov, kombinacije črk in številk in služi za dvig ravni zaupanja uporabnikovega Rekono računa na ustrezno raven zaupanja, ki zadostuje za

	uporabnikovo prijavo v spletno ali mobilno banko Identifikacijski ključ se uporabniku izda ob oddaji vloge in vklopu spletne ali mobilne banke ob osebni identifikaciji v banki in pošlje na e-poštni naslov in mobilno telefonsko številko, ki sta navedena na zahtevku za vklop spletne ali mobilne banke. Identifikacijski ključ poveže uporabnika banke z njegovim Rekono računom. Identifikacijski ključ se uporabniku izda in pošlje ob oddaji vloge in vklopu spletne ali mobilne 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 ali mobilno banko. Uporabnik bo ob prijavi v spletno ali mobilno banko pozvan, naj uporabi oz. vpiše identifikacijski ključ le, če raven zaupanja v njegov Rekono račun še ne zadostuje za prijavo v spletno ali mobilno banko, v nasprotnem identifikacijskega ključa ni potrebno uporabiti. Stranka lahko nov identifikacijski ključ pridobi ob osebni identifikaciji v banki. Uporabi ga lahko, če je ustvarila povsem nov Rekono račun s svojo davčno številko, s katerim se želi prijaviti v spletno ali mobilno banko (prejšnji Rekono račun pa iz različnih razlogov izbrisala). Identifikacijski ključ je veljaven 72 ur od izdaje.
Naročilo	je zahteva za izvedbo bančne storitve, ki jo uporabnik po uspešni avtentikaciji in avtorizaciji pošlje banki z uporabo DBP.

III. Pridobitev pravice za uporabo DBP

3. člen

Uporabnik mora za uporabo spletne ali mobilne banke sam in 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 ali mobilne banke ustvariti Rekono račun (neposredno na www.rekono.si ali pa v samem postopku aktivacije oz. prijave v spletno ali mobilno banko).

Minimalne 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 imetniku transakcijskega, varčevalnega ali kartičnega računa odobri uporabo spletne ali mobilne banke, če so izpolnjeni naslednji pogoji:

- odda v celoti pravilno izpolnjen in podpisan Zahtevek za uporabo spletne ali mobilne banke v katerikoli poslovalnici N Banka d.d.,
- poravna vse stroške, povezane z vklopom spletne ali mobilne banke,
- je star najmanj 18 let in je opravilno sposoben oziroma je star najmanj 15 let in ima soglasje zakonitega zastopnika za samostojno in prosto razpolaganje s sredstvi na svojem računu oziroma je star najmanj 15 let in je v rednem delovnem razmerju ali je pred polnoletnostjo pridobil polno poslovno sposobnost (s sklenitvijo zakonske zveze ali je postal roditelj in je bilo o tem odločeno v nepravdnem postopku) o čemer predloži ustrezno dokumentacijo,
- ima ustrezno napravo z dostopom do interneta, ki omogoča vstop v spletno ali mobilno banko.

Banka pooblaščencu ali zakonitemu zastopniku odobri uporabo spletne ali mobilne banke, če so izpolnjeni naslednji pogoji:

- imetnik računa ima pri banki odprt transakcijski, varčevalni ali kartični račun,
- odda v celoti pravilno izpolnjen in podpisan Zahtevek za uporabo spletne ali mobilne banke v katerikoli poslovalnici N Banka d.d.,
- poravna vse stroške, povezane z vklopom spletne ali mobilne banke,
- predloži pooblastilo imetnika računa za uporabo DBP ozirom odločbo pristojnega organa ali drug ustrezen dokument, iz katerega izhaja, da je zakoniti zastopnik oziroma skrbnik imetnika računa,
- ima ustrezno napravo z dostopom do interneta, ki omogoča vstop v spletno ali mobilno banko.

S podpisom zahtevka ali potrjenega naročila imetnik transakcijskega, varčevalnega ali kartičnega računa, zakoniti zastopnik oziroma pooblaščenec potrjuje, da je seznanjen z določili teh splošnih pogojev in z določili Tarife ter da mu je znano, da sta navedena akta sestavni del pogodbenega razmerja za uporabo spletne ali mobilne banke.

5. člen

Ob vklopu storitve spletne ali mobilne banke banka imetniku računa zaračuna pristopnino. Skladno z vsakokrat veljavno Tarifo nadomestil za storitve banke imetniku računa zaračuna tudi naročnino, ki začne teči s prvim dnem naslednjega meseca, v katerem je uporabnik oddal zahtevek za uporabo spletne ali mobilne banke.

Vsa nadomestila se poravnajo z neposredno bremenitvijo transakcijskega ali kartičnega računa imetnika transakcijskega, varčevalnega ali kartičnega računa s čimer uporabnik s sprejetjem teh splošnih pogojev soglaša.

6. člen

Po plačilu pristopnine banka uporabniku vklopi storitev spletne ali mobilne banke in izda ustrezne avtentikacijske elemente (identifikacijski ključ za dvig ravni zaupanja v Rekono račun), ki jih uporabniku posreduje na elektronski naslov in mobilno telefonsko številko. Uporabnik identifikacijski ključ ob prijavi v spletno ali mobilno banko uporabi za dvig ravni zaupanja v Rekono račun. Z Rekono računom ustrezne ravni zaupanja uporabnik aktivira oz. se lahko prijavi v spletno ali mobilno banko.

7. člen

Pogodba o uporabi spletne oziroma mobilne banke je sklenjena, ko imetnik transakcijskega, varčevalnega ali kartičnega računa oziroma njegov zakoniti zastopnik in banka podpišeta Zahtevek za uporabo spletne ali mobilne banke, ali oddata vlogo za vklop digitalne bančne poti prek drugega varnega kanala (npr. vklop na daljavo). V primeru pooblaščenca se šteje, da je pogodba o uporabi spletne ali mobilne banke sklenjena, ko Zahtevek za uporabo spletne ali mobilne banke podpišejo imetnik transakcijskega ali kartičnega računa, pooblaščenec in banka.

Uporabnik po sklenitvi pogodbe in vklopu ter aktivaciji spletne ali mobilne banke lahko začne z uporabo spletne ali mobilne banke.

8. člen

Banka si pridružuje pravico, da Zahtevek za uporabo spletne ali mobilne banke zavrne brez navedbe razlogov za zavrnitev, o čemer nemudoma, oziroma najkasneje v petih delovnih dneh od prejema vloge, obvesti imetnika transakcijskega, varčevalnega ali kartičnega računa oziroma njegovega zakonitega zastopnika.

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

9. člen

Možni načini in uporaba dostopa do spletne oz. mobilne banke so navedeni v uporabniških navodilih.

10. člen

Možni načini potrjevanja plačilnih nalogov, naročil in spreminjanja nastavitev v spletni banki so navedeni v Navodilih za uporabnike Spletne N Banke.

V. Uporaba storitev DBP

11. člen

Digitalne bančne poti (spletna oziroma mobilna banka) so način opravljanja bančnih storitev prek spleta ali aplikacije, ki uporabnikom glede na vrsto in možnost posameznega računa, omogoča izvajanje naslednjih aktivnosti:

- transakcijski račun: uporabniku omogoča pregled stanja in prometa na računu, plačilnih karticah, varčevanjih in kreditih, izvajanje plačil, naročil, prenosov sredstev med računi v banki, opravljanje menjalniških poslov ter izvajanje drugih storitev, ki jih spletna ali mobilna banka omogoča,
- kartični račun: uporabniku omogoča pregled stanja in prometa na kartičnem računu, izvajanje naročil ter izvajanje drugih storitev, ki jih spletna ali mobilna banka omogoča.

Več informacij o spletni ali mobilni banki je objavljenih na spletnem mestu N Banke in uporabniških navodilih.

Spletna in mobilna banka sta uporabnikom na voljo v slovenskem in angleškem jeziku.

Izvajanje plačilnih nalogov preko spletne ali mobilne banke se ureja v skladu z Urnikom izvrševanja plačilnih transakcij pri banki in Splošnimi pogoji za opravljanje plačilnih storitev preko transakcijskega računa za potrošnike, ki sta sestavni del teh splošnih pogojev in objavljena na spletni strani banke www.nbanka.si ter v vseh poslovalnicah banke.

12. člen

Uporabnik lahko v mobilni banki uporablja **generator enkratnih gesel** mŽeton **za avtentikacijo plačil prek spleta z bančno kartico** in za avtentikacijo pri naročanju **bančnih storitev (kot npr.** vklop spletne banke**)** na daljavo prek spleta.

13. člen

Banka si pridržuje pravico uvajanja novih storitev spletne ali mobilne banke, o čemer bo uporabnika obveščala na spletnih straneh banke, v spletni in mobilni banki ter v vseh poslovalnicah banke.

Postopek dostopa ter način uporabe posamezne Digitalne bančne poti so opisani v uporabniških navodilih, ki so dostopna na spletnih straneh banke in v vseh poslovalnicah banke.

VI. Dolžnosti uporabnika

14. člen

Uporabnik se obvezuje, da:

- bo pri uporabi spletne ali mobilne banke in ustvarjanju in uporabi Rekono računa upošteval poleg teh splošnih pogojev, Splošnih pogojev za opravljanje plačilnih storitev preko transakcijskega računa za potrošnike, drugih splošnih pogojev in pogodb, ki so kakorkoli povezani ter urejajo opravljanje storitev DBP in uporabniških navodil tudi splošne pogoje za uporabo storitve Rekono ter veljavno zakonodajo. Uporabnik bo skrbno hranil naprave, preko katerih bo dostopal do spletne banke oziroma na katerih je nameščena mobilna banka ter vse možne tipe dostopa in avtentikacijske elemente in jih varoval kot dober gospodar,
- bo preprečil izgubo, krajo ali zlorabo gesla, PIN kode, biometrične značilnosti ali elementov in naprav za avtentikacijo 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 ali na katerih je nameščena mobilna banka, uporabniško ime, vstopno geslo, podatek drugega avtentikacijskega faktorja, PIN koda, biometrična značilnost ali identifikacijski ključ; oz. uporabile te elemente za nepooblaščeno uporabo Rekono računa;
- bo pri prijavi v Rekono račun v okviru prijave v spletno ali mobilno vedno vedno preveril, da se v Rekono račun prijavlja na spletnem naslovu https://idp.rekono.si;
- bo v primeru uporabe biometrične značilnosti za prijavo v mobilno banko, na mobilni napravi hranil le lastne biometrične značilnosti. V nasprotnem primeru za vso škodo, ki bi nastala zaradi morebitnih zlorab, odgovarja izključno uporabnik. N Banka ne prevzema odgovornosti za morebitno škodo, ki bi nastala zaradi morebitnih zlorab kot posledica neupoštevanja navodil, povezanih z uporabo biometričnih značilnosti, zapisanih v teh splošnih pogojih in Navodilih za uporabnike Spletne N Banke in Navodilih za uporabnike Mobilne N Banke;
- bo skrbno izbral programsko opremo, ki jo namešča na svoje naprave v izogib zlonamerni programski opremi (virusi, trojanski konji, ipd), da bo imel na svojih napravah nameščen antivirusni program, ter da naprave ne bodo imele omogočenega korenskega dostopa (npr. root, jailbreak, ipd.). Seznam priporočenih antivirusnih programov je objavljen na spletnem mestu banke https://www.nbanka.si/spletna-banka/nacin-dostopa-in-varnost ter na https://www.cert.si/si/zascita/protivirusna-zascita/;
- bo Rekono račun oz. spletno ali mobilno banko ob prejemu aktivacijskih oz. identifikacijskih elementov nemudoma aktiviral;
- bo naprave, na katerih dostopa do Rekono računa oz. spletne ali mobilne banke, zavaroval z avtentikacijskimi elementi, ki so drugačni, kot jih uporablja za Rekono račun oz. spletno ali mobilno banko. Pri kreiranju vstopnih gesel do naprave oz. spletne ali mobilne banke pa bo upošteval priporočila za kvalitetno geslo (8 znakov, velike in male črke, številke….). Dostop do naprav bo uporabnik zaščitil s funkcijo samodejnega zaklepanja (auto lock) in uporabo dostopnega gesla (passcode) in uporabil vse sodobne načine zaščite in tehnologije, objavljene na spletni strani banke ter na https://www.cert.si/si/zascita/;
- naprav ne bo nikoli puščal nenadzorovanih z aktivno spletno ali mobilno banko, oziroma se bo vsakokrat ob zaključku uporabe spletne ali mobilne 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 (mobilna aplikacija Rekono OnePass, varnostni ključ) za avtentikacijo, 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 zaščitil še z drugim avtentikacijskim faktorjem, če je to možno, kot je npr. možno pri ponudniku Gmail).

- bo takoj obvestil banko o morebitni nepooblaščeni uporabi, sumu nepooblaščene uporabe oziroma možnosti nepooblaščene uporabe (npr. če je tretja oseba kakor koli izvedela za avtentikacijski element), kraji ali izgubi naprav preko katerih dostopa do spletne banke oziroma na katerih je nameščena mobilna banka;
- bo v primeru izgube, kraje, zlorabe ali suma na krajo ali zlorabo naprav, preko katerih dostopa do spletne ali mobilne banke ali Rekono računa, to takoj prijavil policiji;
- bo posredoval banki vse potrebne informacije o okoliščinah, povezanih z izgubo, krajo ali zlorabo naprav, preko katerih dostopa do spletne ali mobilne banke, da se prepreči nadaljnje nastajanje škode;
- bo spremljal obvestila o novih različicah in posodobitvah spletne ali mobilne banke;
- bo 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 storitev spletne ali mobilne banke;
- 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 podatkov do spletne ali mobilne banke oz. svojega osebnega Rekono računa; temveč bo avtentikacijske podatke (uporabniško ime, vstopno geslo ipd.) ob vsaki prijavi vpisal v aplikacijo.
- v primeru, da kot drugi faktor prijave v Rekono račun uporabnik uporablja kvalificirano digitalno potrdilo, nameščeno na napravi oz. v brskalniku, bo dostop do kvalificiranega digitalnega potrdila oz. uporabe le-tega, dodatno zaščitil z posebnim geslom.
- bo v primeru suma kraje ali zlorabe ter v primeru izgube naprav, preko katerih dostopa do spletne banke ali na kateri je nameščena mobilna banka, ali suma kraje ali zlorabe kateregakoli od avtentikacijskih elementov, ki se uporabljajo za dostop do spletne ali mobilne banke (uporabniško ime, e-poštni naslov, vstopno geslo, bančna kartica, mobilna telefonska številka 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 oz. mobilne banke oz. deaktivacijo mobilne banke na mobilni napravi, ki je bila odtujena ali izgubljena ter, če je potrebno, blokado tistih avtentikacijskih elementov, ki ji lahko blokira banka (npr. bančna kartica). Za blokado drugih avtentikacijskih elementov, ki niso v domeni banke (npr. SIM kartica, dostop do e-poštnega naslova ipd.), poskrbi uporabnik sam;
- bo ob nepooblaščeni uporabi ali ob sumu oz. možnosti nepooblaščene 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;
- bo ob sumu kraje ali izgube plačilne kartice ter verjetnosti, da je z njegovo PIN kodo seznanjena nepooblaščena 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 www.nbanka.si. Banka ali servisni center bosta blokirala kartico in s tem nadaljnjo uporabo kartice za dostop s to kartico do Spletne N Banke ali za nepooblaščeni dostop do njegovega Rekono računa (oz. Rekono e-identitete). 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 debetne Mastercard in Ide@l Mastercard plačilne kartice, objavljenimi na spletni strani banke https://www.nbanka.si/pripomocki/pogoji-poslovanja/splosni-pogoji-in-placilni-promet;
- bo iz mobilne naprave izbrisal aplikacijo mobilna banka oziroma jo deaktiviral, če naprave ne bo več uporabljal;
- bo ob zamenjavi mobilne naprave, na kateri je nameščena mobilna banka, napravo, v skladu z Navodili za uporabnike Mobilne N Banke, ustrezno deaktiviral, hkrati pa uporabo mobilne banke aktiviral na novi mobilni napravi, z uporabo Rekono računa;
- bo takoj spremenil vstopno geslo ali PIN kodo, po postopku, objavljenem v uporabniških navodilih, oz. bo takoj spremenil avtentikacijske elemente Rekono računa v primeru, da je zanj izvedela tretja oseba;
- pri uporabi spletne ali mobilne banke ne bo uporabljal računalniških kod, škodljivih programov ali česarkoli, kar bi lahko motilo, onesposobilo ali škodovalo uporabi spletne ali mobilne banke, njegovi programski ali strojni opremi ali elektronskem komunikacijskem omrežju; če uporabnik s svojim ravnanjem povzroči škodo, zanjo v celoti odgovarja, tako banki, kot tudi operaterju;
- ne bo uporabljal funkcij »auto-fill« na napravah, preko katerih vstopa v spletno banko oziroma na mobilnih napravah za vpisovanje uporabniškega imena in gesel za svojo mobilno banko;
- ne bo odgovarjal na e-pošto in SMS sporočila, ki jih ni pričakoval s strani banke;
- bo pred izvedbo prijave v spletno banko vsakič preveril, da je na pravem spletnem naslovu »https://e.nbankak.si/«, ter da je vzpostavljena varna povezava na HTTPS protokolu, torej da se spletni naslov spletne banke prične s »https://« in ne »http://«. V primeru, da uporabnik naleti na spletno stran spletne banke, ki deluje kot lažna ali ima v naslovu »http://« in ne »https://«, bo o tem nemudoma obvestil banko.
- ne bo klikal na nobeno povezavo ali drugo obliko teksta, ki je bil poslana preko e-pošte ali v SMS obliki in obstaja možnost, da sporočilo ni bilo poslano s strani banke;

- se bo pri uporabi spletne ali mobilne banke povezoval samo z »zaupanja« vrednimi WiFi omrežji, ki jih bo onemogočil, ko jih ne bo uporabljal (enako velja tudi za Bluetooth povezavo);
- nameščal mobilne aplikacije samo z zaupanja vrednih lokacij (Apple App Store, Google Play, Huawei App Gallery,…);
- ne bo delil podatkov o svoji spletni ali mobilni banki z drugimi uporabniki oziroma tretjimi osebami;
- bo zagotavljal sredstva na računu za svoje poslovanje prek spletne ali mobilne banke;
- bo banko takoj obvestil o vseh nepravilnostih v zvezi z delovanjem storitev spletne ali mobilne banke;
- bo prevzel vso odgovornost za vse posle, ki jih odda prek spletne ali mobilne 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 takoj po prejemu izpiska preveril vse izvedene plačilne storitve in ali je začetno stanje sredstev v posamezni valuti na računu enako končnemu stanju sredstev na osebnem ali kartičnem računu na predhodnem izpisku in najpozneje osmi delovni dan po prejemu izpiska banko obvestil, če obstaja kakršna koli nepravilnost v zvezi s plačilnimi storitvami ali če izpiska ni prejel;
- bo vsako spremembo svojega elektronskega naslova ali spremembo mobilne telefonske številke sporočil banki, v katerikoli poslovalnici banke, z uporabo za to namenjenega obrazca;
- bo vsako spremembo naslova bivališča nemudoma sporočil banki v katerikoli poslovalnici banke, pri čemer se domneva, da je bil izpisek, bančno obvestilo ali sporočilo pravilno poslano in sporočeno uporabniku, če je bilo posredovano na zadnji sporočeni naslov;
- bo vsaj enkrat na mesec prebral obvestila, ki mu jih banka posreduje ob uporabi storitev spletne ali mobilne banke;
- bo ukinil uporabo spletne ali mobilne banke v skladu s 23. členom teh splošnih pogojev, če se ne bo strinjal s spremembami in/ali dopolnitvami določb v teh splošnih pogojih, Tarifo ali z uporabniškimi navodili.

Uporabnik izjavlja, da je uporabnik elektronskega naslova in mobilne telefonske številke, ki ju je navedel na Zahtevku za uporabo spletne banke ali Zahtevku za uporabo mobilne banke ter soglaša s prejemom avtentikacijskih podatkov oziroma identifikacijskega ključa za dvig ravni zaupanja v Rekono račun in aktivacijo spletne ali mobilne banke na navedeni elektronski naslov in mobilno telefonsko številko.

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 zglasiti v katerikoli poslovalnici banke in zahtevati ponovno pošiljanje identifikacijskega ključa.

Uporabnik nosi odgovornost za izbiro, uporabo in vzdrževanje varnostnega sistema za zaščito svojega računalnika, prek katerega dostopa do spletne banke. Uporabnik v celoti odgovarja za vso škodo, ki bi nastala njemu ali banki zaradi zlonamerne kode v njegovem računalniku (računalniški virus) ali zaradi druge zlorabe ali nepooblaščene uporabe spletne ali mobilne banke z njegovimi avtentikacijskimi sredstvi.

V primeru dvomov v identiteto spletne strani storitve spletne banke mora uporabnik le-to preveriti prek znaka »VeriSign Secured Seal« ki potrjuje identiteto strani.

VII. Dolžnosti banke

15. člen

Banka se zavezuje, da bo:

- naloge za izvedbo plačilne transakcije, opravljene preko spletne ali mobilne banke in druge bančne storitve, ki jih uporabnik uporablja v spletni ali mobilni banki, izvršila v skladu Splošnimi pogoji opravljanja plačilnih storitev preko transakcijskega računa za potrošnike in drugimi splošni pogoji za posamezno storitev ter pogodbami, ki jih ima banka sklenjene z uporabnikom ter vsakokrat veljavno zakonodajo,
- svoje obveznosti izvrševala v skladu s pogodbo, temi splošnimi pogoji ter z vsemi drugimi splošnimi pogoji, ki jih je uporabnik sklenil z banko in so kakorkoli povezane ter urejajo opravljanje te storitve,
- uporabnika prek spletne ali mobilne banke obvestila o morebitni zavrnitvi izvršitve plačilne transakcije,
- o vsaki spremembi oziroma dopolnitvi teh splošnih pogojev ter Tarife nadomestil za storitve banke obvestila uporabnika, vsebina omenjenih aktov pa bo dostopna v poslovalnicah banke ter na spletni strani,
- pri uporabi spletne ali mobilne banke računalniško zapisovala vse postopke, ki jih opravi uporabnik spletne ali mobilne banke (vstop in izstop v spletno ali mobilno banko ter datum in čas oddaje plačilnih transakcij) in bo skladno z obstoječo zakonodajo skrbela za ustrezno hrambo teh zapisov,
- obveščala uporabnika o novostih pri uporabi spletne ali mobilne banke,
- obveščala uporabnika o novih verzijah spletne ali mobilne banke.

16. člen

Banka si bo prizadevala, da bo uporaba spletne in mobilne banke dostopna ves čas, čeprav je mogoče, da bo včasih kakovost storitve oziroma dostop do storitve otežen ali onemogočen zaradi vzrokov zunaj njenega nadzora. Za dostopnost avtentikacijskega sistema Rekono je odgovoren ponudnik storitve Rekono.

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

17. 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 na, 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 ali mobilne banke. Banka ne odgovarja za škodo, ki bi nastala zaradi izpada razpoložljivosti storitve Rekono.

Banka tudi ne odgovarja za težave pri uporabi spletne ali mobilne banke, če na strani uporabnika ni zadoščeno tehničnim pogojem za uporabo spletne ali mobilne banke.

Banka ne odgovarja za škodo, ki bi nastala kot posledica napačnega ravnanja ali napačnega posredovanja podatkov uporabnika spletne ali mobilne banke.

Odgovornost banke za morebitno škodo je omejena le na navadno škodo. Banka ne odgovarja za škodo iz naslova izgubljenega dobička ali za nepremoženjsko škodo.
Vse prijave in poskusi prijav v spletno ali mobilno banko (ter postopki pooblaščencev in zakonitih zastopnikov znotraj spletne ali mobilne banke DBP) se beležijo. Omenjene podatke banka hrani v skladu z veljavno zakonodajo.

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 uporabnika

18. člen

Če v teh splošnih pogojih ni določeno drugače, uporabnik spletne ali mobilne banke krije celotno izgubo zneska neodobrene plačilne transakcije in pripadajočih nadomestil ter obresti, če je izvršitev neodobrene plačilne transakcije:

- posledica prevare in/ali goljufije uporabnika spletne ali mobilne banke ali če uporabnik spletne ali mobilne banke naklepno ali zaradi hude malomarnosti ni izpolnil svojih obveznosti v zvezi z ukrepi za zaščito dostopov in naprav, s katerimi dostopa do spletne ali mobilne banke, v skladu s določili teh splošnih pogojev in uporabniških navodil ter v zvezi z ukrepi za zaščito avtentikacijskih podatkov na napravi, preko katere dostopa do spletne ali mobilne banke skladno s temi splošnimi pogoji,
- posledica kršitve teh splošnih pogojev s strani uporabnika spletne ali mobilne banke.

Uporabnik spletne ali mobilne banke krije izgubo zneska neodobrene plačilne transakcije v spletni ali mobilni banki in pripadajočih nadomestil ter obresti do največ 50,00 EUR, če je izvršitev neodobrene plačilne transakcije v spletni ali mobilni banki posledica:

- zlorabe ukradenih ali izgubljenih varnostnih elementov, od trenutka ko je banki prijavil krajo, izgubo ali zlorabo in je banki sporočil vse potrebne podatke za izvedbo blokade, ter če zloraba ni nastala zaradi naklepa ali hude malomarnosti uporabnika,
- ukradene ali izgubljene naprave (kot npr. zloraba vstopnega gesla, kraja ali izguba identifikacijskega ključa, itd),
- naprave, ki je bila zlorabljena, če uporabnik spletne ali mobilne banke ni zavaroval osebnih varnostnih elementov plačilnega instrumenta skladno s temi splošnimi pogoji.

Če je uporabnik upravičen do povračila zneska plačilnih transakcij, bo banka takoj, razen če bo zaradi okoliščin posameznega primera potrebovala daljši rok (o čemer bo uporabnika nemudoma obvestila), znesek plačilnih transakcij nakazala na uporabnikov račun.

19. člen

Če uporabnik sumi, da je bil avtentikacijski element prestrežen, zlorabljen, ukraden ali je bila z njim seznanjena tretja oseba, ali mu je bila ukradena naprava preko katere dostopa do spletne ali mobilne banke, mora:

- obvestiti banko na način in v skladu s temi splošnimi pogoji,
- takoj vložiti zahtevek za izdajo novih avtentikacijskih oz. identifikacijskih elementov,
- zahtevati blokado avtentikacijskih ali identifikacijskih elementov in naprave, za katero velja sum zlorabe,
- takoj zamenjati avtentikacijske elemente.

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

20. člen

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

IX. Začasna ustavitev uporabe DBP

21. člen

Banka začasno onemogoči dostop do spletne ali mobilne banke, kadar:
- uporabnik doseže določeno število napačnih prijav z avtentikacijskimi elementi (skladno z uporabniškimi navodili),
- uporabnik prijavi izgubo, krajo ali nepooblaščen dostop do naprave preko katere dostopa do spletne ali mobilne banke in/ali enega izmed možnih dostopov do spletne ali mobilne banke,
- obstaja sum o možnosti nepooblaščenega dostopa do spletne ali mobilne banke.

Banka o začasno onemogočenem dostopu do spletne ali mobilne banke iz razlogov, navedenih v prvi alineji prvega odstavka tega člena, uporabnika seznani na vstopnem zaslonu spletne banke takoj ob naslednjem poskusu vstopa v spletno banko oziroma neposredno v mobilni banki.

Banka o začasnem onemogočanju dostopa do spletne ali mobilne banke iz razlogov, navedenih v tretji in četrti alineji prvega odstavka tega člena, uporabnika seznani po elektronski pošti in/ali preko SMS sporočil, na e-poštni naslov in/ali številko mobilnega telefona, ki ju je uporabnik navedel na Zahtevku za uporabo spletne ali mobilne banke in/ali na spletnem mestu banke. Odprava začasnega onemogočanja dostopa do mobilne banke se izvede, ko so odpravljeni vsi razlogi začasne ustavitve uporabe in ko uporabnik odda zahtevek za odstranitev blokade mobilne banke.

Uporabnik uredi ponovni dostop do spletne ali mobilne banke v skladu z uporabniškimi navodili, glede na vrsto onemogočenega dostopa.

22. člen

Plačilni nalogi v čakalnici spletne ali mobilne banke, ki se v čakalnici nahajajo v trenutku začasne ustavitve uporabe spletne ali mobilne banke, se izvedejo ne glede na začasno onemogočenje uporabe, če so izpolnjeni pogoji za njihovo izvršitev.

X. Obveščanje uporabnikov

23. člen

Uporabnik se lahko v spletni banki naroči na prejemanje brezplačnih e-poštnih in/ali SMS obvestil, glede na kriterije, ki jih določi na spletni banki, na svoj e-poštni naslov ali številko mobilnega telefona, ki ju je uporabnik navedel na Zahtevku za uporabo spletne banke.

Uporabnik je odgovoren za navedbo pravilnih kontaktnih podatkov. Banka se zavezuje, da bo 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.

Uporabnikom so navodila, obvestila in informacije o spletni banki na voljo tudi na spletnih straneh banke.

XI. Ukinitev uporabe DBP

24. člen

Uporabnik lahko kadarkoli preneha uporabljati storitev, ki jo opredeljujejo ti splošni pogoji, kar stori tako, da pisno ukine uporabo spletne ali mobilne banke. To stori z obrazcem Zahtevek za ukinitev uporabe Spletne N Banke ali z obrazcem Zahtevek za ukinitev uporabe Mobilne N Banke (v nadaljevanju Zahtevek za ukinitev spletne ali mobilne banke), ki ga odda v poslovalnici banke. Banka ukine uporabo nemudoma oziroma najpozneje v petih (5) delovnih dneh po prejemu uporabnikovega Zahtevka za ukinitev spletne ali mobilne banke.

Oddaja zahtevka za ukinitev spletne ali mobilne banke ne pomeni takojšnje blokade uporabe spletne ali mobilne banke. Če obstaja potreba po takojšnji blokadi spletne ali mobilne banke (npr. če obstaja sum zlorabe), stranka zahteva blokado na druge načine, ki so opisani v teh splošnih pogojih.

25. člen

Uporabnik je dolžan pred datumom ukinitve uporabe spletne ali mobilne banke sam poskrbeti za predčasno izvršitev vseh plačilnih transakcij v čakalnici (čakalni vrsti) ali preklic njihove izvršitve. V primeru, da uporabnik plačilnih transakcij v čakalnici ni preklical, se te izvedejo v skladu z Urnikom izvrševanja plačilnih transakcij pri banki.
Vse obveznosti uporabnika, nastale do dneva ukinitve uporabe spletne ali mobilne banke, se, ne glede na prenehanje, izvršijo v skladu z določili teh splošnih pogojev.

Odpoved oz. ukinitev uporabe digitalne bančne poti pri N Banki banki pomeni, da banka zapre oz. izklopi servis spletne ali mobilne banke ter prijava vanj z aktivnim Rekono računom ni več možna. Ukinitev uporabe spletne ali mobilne banke ne pomeni tudi ukinitve Rekono uporabniškega računa.

26. člen

Banka lahko uporabniku ukine spletno ali mobilno banko, v naslednjih primerih:

- če uporabnik poda Zahtevek za ukinitev spletne ali mobilne banke,
- če uporabnik banki ali banka uporabniku odpove Okvirno pogodbo o odprtju in vodenju transakcijskega računa, na katerega je vezana spletna ali mobilna banka, skladno s Splošnimi pogoji za opravljanje plačilnih storitev preko transakcijskega računa za potrošnike,
- 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 tako zahteva zakonodaja ali pristojni organ,
- če uporabnik odpove Pogodbo o okvirnem kreditu na posojilni Ide@l Mastercard kartici, v primeru, da do spletne ali mobilne banke dostopa samo kot imetnik kartičnega računa, odprtega pri N Banki.

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

XII. Pomoč uporabnikom

27. člen

Pomoč za nemoteno in pravilno uporabo spletne ali mobilne banke zagotavlja Kontaktni center banke na brezplačni telefonski številki 080 22 65, ki je uporabniku dosegljiv v okviru urnika poslovanja, ki je objavljen na spletni strani banke www.nbanka.si.

XIII. Nadomestila in stroški

28. člen

Banka imetniku transakcijskega ali kartičnega računa oziroma uporabniku za najem, uporabo spletne ali mobilne banke in opravljene plačilne transakcije zaračunava nadomestila in stroške v skladu z vsakokrat veljavno Tarifo nadomestil za storitve banke.

Banka svoje terjatve poravna z bremenitvijo transakcijskega in/ali kartičnega računa imetnika transakcijskega ali kartičnega računa oziroma uporabnika, o čemer ga obvesti z izpiskom in s čimer imetnik transakcijskega ali kartičnega računa oziroma zakoniti zastopnik oziroma uporabnik soglaša s sprejetjem teh splošnih pogojev.

Tarifa je na voljo v vsaki poslovalnici banke in na spletni strani banke.

29. člen

Uporaba spletne ali mobilne banke v mesecu, ko je imetnik transakcijskega ali kartičnega računa oziroma zakoniti zastopnik oziroma uporabnik oddal Zahtevek za uporabo spletne ali mobilne banke, je brezplačna. Banka imetniku transakcijskega ali kartičnega računa oziroma uporabniku mesečno naročnino začne zaračunavati s prvim dnem naslednjega meseca. Uporaba spletne ali mobilne banke v mesecu ukinitve je prav tako brezplačna.

XIV. Pritožbe, reklamacije

30. člen

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 ali spletnega obrazca.

31. člen

Morebitne spore ali pritožbe v zvezi z opravljanjem storitev v skladu s temi splošnimi pogoji bosta uporabnik in banka reševala sporazumno v skladu z vsakokrat veljavnim 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 www.nbanka.si. 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 spletni strani banke ter na drugi stopnji (pritožba na Komisijo za pritožbe) pisno – po pošti, na naslov sedeža banke.

XV. Varovanje podatkov in splošne določbe

32. člen

Banka bo osebne podatke uporabnika hranila in varovala na način, tako da ne bo prišlo do morebitnih neupravičenih razkritij podatkov nepooblaščenim osebam, na način, kot določeno v vsakokrat veljavnih Splošnih informacijah o varstvu osebnih podatkov, dostopnih tudi na www.nbanka.si/varstvo-osebnih-podatkov. Z vsebino navedenega dokumenta in možnostjo pridobitve le tega v tiskani obliki, banka seznani Uporabnika ob oddaji Zahtevka za uporabo spletne ali mobilne banke.

33. člen

Banka in uporabnik se zavezujeta, da bosta v obojestranskem interesu zagotavljala visoko varnost poslovanja prek spletne in mobilne banke in se tako izogibala tveganju neavtoriziranega pristopa do podatkov, spreminjanja podatkov in izgube podatkov.

XVI. Končne določbe

34. člen

V primeru sprememb in/ali dopolnitev splošnih pogojev, banka seznani uporabnika pisno z izpiski, prek spletnega mesta www.nbanka.si, spletne ali mobilne banke ali na drug ustrezen način, dva meseca pred uveljavitvijo spremenjenih in/ali dopolnjenih splošnih pogojev, in sicer tako, da mu pošlje predlog spremembe in/dopolnitev splošnih pogojev.

Če se uporabnik s spremembami in/ali dopolnitvami splošnih pogojev ne strinja, lahko brez odpovednega roka in plačila nadomestil zahteva ukinitev spletne ali mobilne banke, sklenjene na podlagi teh splošnih pogojev. Enako velja tudi za spremembe in dopolnitve Tarife nadomestil za storitve banke.

Odstop od pogodbe mora uporabnik podati najkasneje do konca dneva pred določenim dnem začetka veljavnosti sprememb in/ali dopolnitev splošnih pogojev, kar stori z Zahtevkom za ukinitev spletne ali mobilne banke za fizične osebe v poslovalnici banke. Če uporabnik v tem roku banki ne sporoči, da se s spremembami in/ali dopolnitvami ne strinja, se šteje, da s spremembami in/ali dopolnitvami splošnih pogojev soglaša.

V primeru, če uporabnik zavrne predlagane spremembe in pri tem ne zahteva ukinitev spletne ali mobilne banke, na način, da odda Zahtevek za ukinitev spletne ali mobilne banke, se šteje, da je banka odpovedala pogodbo z dvomesečnim odpovednim rokom, ki teče od dneva pošiljanja obvestila o spremembi.

Z začetkom veljavnosti teh splošnih pogojev, prenehajo veljati dosedanji splošni pogoji poslovanja za uporabnike Digitalnih bančnih poti.

Za vse Pogodbe o uporabi Spletne N Banke za fizične osebe oziroma Pogodbe o uporabi Mobilne N Banke za fizične osebe, ki so bili sklenjene pred sprejetjem teh splošnih pogojev, veljajo novo sprejeti splošni pogoji, razen, če se uporabnik s spremembami in/ali dopolnitvami ne strinja in poda odstop od pogodbe (v primeru morebitnih razhajanj med določbami Pogodbe o uporabi Spletne N Banke za fizične osebe oziroma Pogodbe o uporabi Mobilne N Banke za fizične osebe in temi splošnimi pogoji, prevladajo določbe slednjih).

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

35. člen

Vsakokrat veljavni splošni pogoji bodo objavljeni na spletni strani banke. Hkrati bodo na voljo v vseh poslovalnicah banke. Ti splošni pogoji so sestavni del Zahtevka za uporabo spletne ali mobilne banke za fizične osebe, ki velja kot pogodba.

Splošni pogoji veljajo od 11.04.2022 in pod pogojem, da se bo takrat pričel prehod na uporabo novih avtentikacijskih načinov Rekono v spletni in mobilni 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 11.04.2022