Splošni pogoji uporabe storitve Rekono

Ljubljana, 15. december 2022

Zaščita dokumenta

Skrbnik dokumenta:	**svetovalec direktorja podjetja Rekono**
Odobritelj dokumenta:	**direktor podjetja Rekono**
Področje veljavnosti:	**delovna področja podjetja Rekono, vezana na izvajanje storitev e-identifikacije Rekono in oddaljenega e-podpisa, e-žiga in časovnega žiga v okviru Rekono.Sign**

KAZALO

1. SPLOŠNO

1. Ti splošni pogoji urejajo uporabo spletne storitve za elektronsko identifikacijo in avtentikacijo Rekono (v nadaljevanju: storitev Rekono), ki jo uporabnikom zagotavlja družba Rekono d.o.o. (v nadaljevanju: »družba Rekono« oz. upravljavec). Uporabnik s sprejetjem splošnih pogojev in registracijo svoje pravne identitete z odprtjem računa v okviru sistema Rekono (v nadaljevanju: račun Rekono) pridobi pravico, da svoj račun Rekono z izbranimi elementi avtentikacije in avtentikacijskim postopkom uporablja v storitvah zaupanja za elektronske transakcije in drugih rešitvah oz. storitvah ponudnikov spletnih in drugih elektronskih storitev, ki za dostop do teh storitev zahtevajo zanesljivo in varno predstavitev in potrditev (avtentikacijo) uporabnikove identitete.

2. Z registracijo in odprtjem računa Rekono uporabnik z družbo Rekono sklene pogodbeno razmerje za uporabo storitev Rekono v skladu s temi splošnimi pogoji in spremljajočimi navodili. Sklenjena pogodba je tudi pravna podlaga za obdelavo uporabnikovih osebnih podatkov v okviru sistema in storitev Rekono, z izjemo podatkov o lokaciji uporabnika storitve Rekono OnePass, za obdelavo katerih ima upravljavec izkazane zakonite interese.

3. Kadar uporabnik račun Rekono odpre v povezavi z začetkom uporabe storitve določenega ponudnika teh storitev (npr. banke, zavarovalnice ali druge finančne organizacije, TK operaterja ipd.), je uporabnik pri uporabi računa Rekono lahko zavezan tudi k spoštovanju dodatnih pogojev, ki jih določi ponudnik te storitve.

4. Politika Rekono.TSP in opisi delovanja storitve Rekono v različicah, veljavnih ob sprejetju splošnih pogojev, so del splošnih pogojev in dostopni na www.rekono.si.

5. Sestavni del teh splošnih pogojev je tudi politika Rekono.TSP, ki je dostopna na https://www.rekono.si/sl/politika-rekono-tsp/

2. IZRAZI IN KRATICE

2.1. Izrazi, uporabljeni v teh splošnih pogojih, pomenijo:

a) »Biometrični podatki« so podatki o fizičnih značilnostih posameznika, kot so na primer prstni odtis, podoba obraza ali roženice, ki jih mobilna naprava zajame s pomočjo vgrajenih senzorjev in obdela za namen avtorizacije posameznika za uporabo dotične mobilne naprave oz. njene kartice SIM. Ti podatki so shranjeni le na posameznikovi mobilni napravi in družba Rekono do njih nima dostopa, uporabijo pa se lahko kot eden od elementov avtentikacije posameznika.

b) »Element avtentikacije« je dejavnik, ki je dokazljivo povezan z osebo, in spada v (najmanj) eno izmed naslednjih kategorij:
   - »element avtentikacije, ki temelji na posesti« (nekaj, kar je v izključni lasti uporabnika), pomeni dejavnik avtentikacije, za katerega mora oseba dokazati, da ga ima v posesti;
   - »element avtentikacije, ki temelji na poznavanju« (nekaj, kar ve samo uporabnik), pomeni dejavnik avtentikacije, za katerega mora oseba dokazati, da ga pozna;
   - »inherentni element avtentikacije« (nekaj, kar uporabnik je) pomeni dejavnik avtentikacije, ki temelji na fizični značilnosti fizične osebe, in v zvezi s katerim mora oseba dokazati, da ima navedeno fizično značilnost.

c) »Rekono OnePass« je mobilna aplikacija za izvedbo močne, dvofaktorske avtentikacije uporabnika z uporabo potisnih obvestil in enkratnih gesel (TOTP).

d) »SMS-OTP« je enkratno geslo, namenjeno prijavi v račun Rekono, s SMS poslano na mobilni telefon uporabnika.

e) »Uporabnik« je fizična oseba, ki račun Rekono uporablja kot posameznik ali kot zastopnik pravne osebe.

f) »Verodostojni vir« je kateri koli vir v poljubni obliki, ki na zanesljiv način zagotavlja natančne podatke, informacije in/ali dokaze, ki se lahko uporabljajo za dokazovanje identitete osebe.

g) »Močna avtentikacija« pomeni avtentikacijo z uporabo dveh ali več elementov, ki spadajo v kategorijo znanja (nekaj, kar ve samo uporabnik), lastništva (nekaj, kar je v izključni lasti uporabnika) in neločljive povezanosti z uporabnikom (nekaj, kar uporabnik je), ki so med seboj neodvisni, kar pomeni, da kršitev enega elementa ne zmanjšuje zanesljivosti drugih, in so zasnovani na tak način, da varujejo zaupnost podatkov, ki se preverjajo.

h) »Varno spletno nakupovanje« je spletno nakupovanje na prodajnih mestih, ki uporabljajo storitev za varno spletno plačevanje na spletnih prodajnih mestih Mastercard SecureCode, Mastercard Identity Check in Visa Secure.

i) »Rekono 3D Secure« pomeni storitev, ki imetnikom plačilnih kartic omogoča varno spletno nakupovanje v sklopu uporabe storitve Mastercard ID Check in Visa Secure (poimenovan tudi 3D Secure 2.0).

Drugi izrazi, uporabljeni v teh splošnih pogojih, imajo enak pomen, kot ga imajo v Uredbi (EU) št. 910/2014 Evropskega Parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja v elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/ES (v nadaljevanju: Uredba eIDAS) v izvedbenih predpisih, izdanih na podlagi Uredbe eIDAS ter v Zakonu o elektronski identifikaciji in storitvah zaupanja (Uradni list RS, št. 121/21 in 189/21 – ZDU-1M).

2.2. Kratice

PAN	številka plačilne kartice (angl. Payment Card Number)
PIN	osebna identifikacijska številka (angl. Personal Identification Number)
TSP	ponudnik storitev zaupanja (angl. Trust Service Provider)
SMS-OTP	enkratna gesla poslana na mobilni telefon
FIDO	odprti standard za avtentikacijo, https://fidoalliance.org/ (angl. Fast IDentity Online)

3. REGISTRACIJA IN UPORABA RAČUNA REKONO

1. Uporabnik pridobi pravico uporabe računa Rekono tako, da se na spletnem mestu www.rekono.si registrira in s klikom na potrditveno polje »Strinjam se s pogoji uporabe« sprejme splošne pogoje ter s tem aktivira račun Rekono.

2. Raven zaupanja v identiteto uporabnika, izkazano in zagotavljano z računom Rekono, je odvisna od postopka registracije in aktivacije računa Rekono, postopka preverjanja in potrditve uporabnikove identitete, uporabljenih elementov avtentikacije, ter od načina upravljanja računa Rekono. Našteti postopki so v storitvi Rekono izvedeni v skladu z zahtevami Uredbe (EU) št. 910/2014 in na njeni podlagi izdane Izvedbene uredbe Komisije (EU) 2015/1502 ter relevantnimi tehničnimi specifikacijami in standardi.

3. Storitev Rekono obsega izdajanje in upravljanje računov Rekono naslednjih ravni zanesljivosti:

a) zelo nizke (0), ki zagotavlja majhno zaupanje v izkazano in zagotavljano identiteto uporabnika in neznatno zmanjšuje nevarnost zlorabe ali spreminjanja uporabnikove identitete;
b) nizke (10), ki zagotavlja omejeno zaupanje v izkazano in zagotavljano identiteto uporabnika, in katere namen je zmanjšati nevarnost zlorabe ali spreminjanja uporabnikove identitete. Ta nivo zanesljivosti je ekvivalenten eIDAS nizke ravni zanesljivosti;
c) srednje (20), ki zagotavlja srednje zaupanje v izkazano in zagotavljano identiteto uporabnika, in katere namen je znatno zmanjšati nevarnost zlorabe ali spreminjanja uporabnikove identitete. Ta nivo zanesljivosti je ekvivalenten eIDAS srednje ravni zanesljivosti;
d) visoke (30), ki zagotavlja višje zaupanje v izkazano in zagotavljano identiteto uporabnika, in katere namen je preprečiti nevarnost zlorabe ali spreminjanja uporabnikove identitete. Ta nivo zanesljivosti je ekvivalenten eIDAS visoke ravni zanesljivosti.

4. V okviru računa Rekono so uporabniku na voljo naslednji elementi avtentikacije:

a) uporabniško ime in geslo – kot uporabniško ime se uporablja elektronski poštni naslov, ki ga določi uporabnik ob registraciji računa Rekono, geslo pa sestavlja niz znakov, ki jih mora uporabnik obvezno določiti ob registraciji računa;
b) potisna obvestila, poslana in potrjena v aplikaciji Rekono OnePass, ki je del storitve Rekono;

c) geselnik za mobilne naprave – tvori časovno spremenljiva enkratna gesla (TOTP). Lahko se uporabi zgolj aplikacija Rekono OnePASS, ki je del storitve Rekono;
d) naprave FIDO – fizična potrditev s kompatibilno napravo FIDO;
e) SMS-OTP – enkratna gesla, poslana na mobilni telefon po SMS;
f) kvalificirano potrdilo – omogočena je registracija in uporaba kvalificiranih potrdil overiteljev, registriranih v Sloveniji.
g) sredstvo elektronske identifikacije ravni visoko, ki je izdano v obliki digitalnega potrdila, shranjenega na čipu osebne izkaznice.

5. Ob registraciji posameznega elementa avtentikacije storitev Rekono vedno izvede potrditev lastništva oziroma posedovanja (proof-of-possession) elementov avtentikacije, ki jih bo uporabljal določeni uporabnik. Potrditev se izvede za vse v prejšnji točki navedene elemente, in sicer:

a) za potrditev posedovanja elektronskega poštnega naslova storitev Rekono uporabniku na ta naslov pošlje elektronsko sporočilo, ki vsebuje kodo za potrditev;
b) za potrditev mobilne aplikacije Rekono OnePass se mora uporabnik prijaviti z računom Rekono in izvesti postopek močne avtentikacije;
c) za potrditev posedovanja mobilnega telefona za SMS-OTP na številko mobilnega telefona, ki jo je v postopku registracije navedel uporabnik, storitev Rekono pošlje enkratno geslo za potrditev posedovanja;
d) za potrditev posedovanja kvalificiranega potrdila se mora uporabnik prijaviti s svojim veljavnim kvalificiranim potrdilom;
e) za potrditev posedovanja naprave FIDO mora uporabnik izkazati lastništvo z aktivacijo naprave.
f) sredstvo elektronske identifikacije ravni visoko, ki je izdano v obliki digitalnega potrdila, shranjenega na čipu osebne izkaznice.

6. Elementi avtentikacije, ki so na voljo v računu Rekono, uporabniku omogočajo močno dvofaktorsko avtentikacijo. Za izkazovanje in zagotavljanje srednje ali visoke ravni zaupanja v svojo identiteto mora uporabnik v svojem računu Rekono:

a) registrirati svoje veljavno kvalificirano potrdilo, ali
b) svojo identiteto potrditi v registracijski pisarni ponudnika storitev zaupanja, ki uporabniku izda kvalificirano potrdilo, ali
c) izvesti registracijo z veljavno kombinacijo številke PAN in PIN svoje bančne kartice, ali
d) izvesti potrditev identitete v registracijski pisarni Rekono.
e) sredstvo elektronske identifikacije ravni visoko, ki je izdano v obliki digitalnega potrdila, shranjenega na čipu osebne izkaznice.

Elementi avtentikacije računa Rekono se lahko uporabljajo izključno za avtentikacijo uporabnika v sistemu Rekono.

7. Za zelo nizko raven zaupanja v uporabnikov račun Rekono zadošča zgolj potrditev lastništva nad sredstvi elektronske identifikacije (e-naslov in telefonska številka), ter strinjanje s splošnimi pogoji.

8. Za nizko raven zaupanja v uporabnikov račun Rekono zadošča potrditev identitete s preverjanjem zunanjih registrov na osnovi podatkov, ki jih posreduje uporabnik.

9. Za srednjo raven zaupanja v uporabnikov račun Rekono zadošča, da se uporabnik registrira:

a) z obstoječim kvalificiranim potrdilom, ali
b) z veljavno kombinacijo številke PAN in PIN svoje plačilne kartice, ki je bila izdana, ko je banka ugotovila in preverila njegovo istovetnost na daljavo, brez osebne navzočnosti, v skladu z določbami zakona, ki ureja preprečevanje pranja denarja in financiranje terorizma, ali
c) s potrditvijo svoje identitete preko zunanjega izvajalca, za katerega je organ za ugotavljanje skladnosti potrdil zanesljivost postopka, ki je enakovreden fizični prisotnosti, ali
d) s potrditvijo svoje identitete preko oddaljene identifikacije v registracijski pisarni Rekono.

Potrditev identitete na načina a) in c) zadošča pogojem za izdajo kvalificiranega potrdila.

10. Za visoko raven zaupanja v uporabnikov račun Rekono mora uporabnik svojo identiteto:

a) potrditi v registracijski pisarni Rekono, ki njegovo istovetnost ugotovi in preveri z vpogledom v njegov uradni identifikacijski dokument s fotografijo ob njegovi osebni navzočnosti ter s preverbo identifikacijskih podatkov v centralnem registru prebivalstva in davčnem registru, ali
b) v svojem računu Rekono registrirati veljavno kvalificirano potrdilo, ki je bilo izdano na napravi za ustvarjanje kvalificiranega elektronskega podpisa, ali
c) registrirati z veljavno kombinacijo mobilne telefonske številke, ki je predhodno vnesena v bančnem sistemu imetnika kartice, številke PAN in PIN svoje plačilne kartice, ki mu jo je izdala banka potem, ko je v skladu z zakonom, ki ureja preprečevanje pranja denarja in financiranje terorizma, njegovo istovetnost ugotovila in preverila z vpogledom v

njegov uradni osebni identifikacijski dokument s fotografijo ob njegovi osebni navzočnosti, ali

d) v svojem računu Rekono registrirati veljavno sredstvo elektronske identifikacije ravni visoko, ki je izdano v obliki digitalnega potrdila, shranjenega na čipu osebne izkaznice.

Potrditev identitete na načine a), b), c) in d) zadošča pogojem za izdajo kvalificiranega potrdila.

11. Uporabniku avtentikacija z računom Rekono, ki zagotavlja srednjo ali visoko raven zaupanja v njegovo identiteto, omogoča, da s storitvijo Rekono.Sign lahko na daljavo ustvari:

a) napredni elektronski podpis;
b) napredni elektronski podpis s kvalificiranim potrdilom;
c) kvalificirani elektronski podpis;
d) napredni ali kvalificirani elektronski žig;
e) napredni ali kvalificirani elektronski časovni žig;
f) preverjanje veljavnosti elektronskega podpisa ali žiga; ter
g) v povezavi z ustvarjanjem elektronskega podpisa, izdajo naprednega in kvalificiranega elektronskega časovnega žiga.

4. VARNO SPLETNO NAKUPOVANJE S STORITVIJO REKONO 3D SECURE

1. Storitev Rekono 3D Secure (v nadaljevanju: Rekono 3D Secure) je storitev za varno potrjevanje spletnih nakupov na spletnih prodajnih mestih, ki je imetniku plačilne kartice na voljo z uporabo mobilne aplikacije Rekono OnePass ali alternativne rešitve Rekono SMS OTP. Za uporabo katere koli od omenjenih rešitev si mora imetnik plačilne kartice registrirati račun Rekono, ki se po vnosu in preverbi podatkov o plačilni kartici nastavi na srednjo ali visoko raven zanesljivosti.

2. Rekono 3D Secure je na voljo uporabnikom računa Rekono, ki so imetniki plačilnih kartic bank, s katerimi ima družba Rekono sklenjen dogovor o zagotavljanju omenjene storitve (v nadaljnjem besedilu: banka). Uporaba Rekono 3D Secure je za vse uporabnike brezplačna.

3. Uporabnik je pri uporabi Rekono 3D Secure poleg teh splošnih pogojev zavezan spoštovati tudi pogoje, ki jih za spletne nakupe z uporabo storitve Mastercard ID Check in Visa Secure določi banka.

4. Imetnik plačilne kartice lahko registracijo računa Rekono izvede v okviru mobilne aplikacije Rekono OnePass ali pa na spletni strani rekono.si, na kateri je na voljo tudi opis postopka registracije.

5. Uporabnik storitev za varno potrjevanje spletnih nakupov aktivira v mobilni aplikaciji Rekono OnePass ali na spletu, preko nadzorne plošče za upravljanje računa Rekono, in sicer tako, da vnese številko ene od svojih plačilnih kartic (PAN) in pripadajočo osebno identifikacijsko številko (PIN). Podatki PIN se v aplikaciji Rekono OnPass ne shranijo, ampak zašifrirajo s šifrirnim ključem procesnega centra, t.j. družbe Bankart, in pošljejo banki, izdajateljici uporabljene plačilne kartice, ki jih tudi shrani.

6. Z aktivacijo ene plačilne kartice se aktivirajo vse uporabnikove plačilne kartice banke izdajateljice aktivirane kartice.

7. V primeru uporabe mobilne aplikacije Rekono OnePass uporabnik za potrditev plačila pri varnem spletnem nakupu prejme potisno obvestilo, s katerim preveri podatke o nakupu in nakup potrdi. Izvedba varnega spletnega nakupa je lahko onemogočena v primeru obstoja dejavnikov, ki predstavljajo visoko tveganje za zlorabe.

8. Za uporabnike, ki nimajo pametnih telefonov, oziroma ki za potrjevanje plačil ne želijo uporabljati mobilne aplikacije Rekono OnePass, je na voljo alternativna rešitev Rekono SMS OTP, kjer uporabnik v postopku potrjevanja nakupa na spletnem prodajnem mestu v brskalnik vnese geslo za spletne nakupe, ki si ga je predhodno nastavil v okviru računa Rekono, in enkratno varno geslo, ki ga prejme v obliki SMS-sporočila na številko mobilnega telefona, s katere je registriral svoj račun Rekono.

9. Pri spletnem nakupu z uporabo storitve Mastercard Identity Check in Visa Secure se imetnik kartice ne predstavi s številko kartice, temveč pristnost svoje identitete potrdi znotraj aplikacije Rekono OnePass ob prejetem potisnem obvestilu o izvedbi varnega spletnega nakupa, ali s svojim geslom za varne spletne nakupe in z enkratnim varnim geslom, ki ga prejme v sporočilu SMS.

10. V primeru uporabe rešitve Rekono SMS OTP mora uporabnik ob vsakem nakupu na spletnem prodajnem mestu, ki podpira uporabo storitve Mastercard in Visa Secure Identity Check, pred izvedbo nakupa vnesti svoje geslo za varne spletne nakupe, ki si ga je nastavil ob vklopu storitve za varne spletne nakupe v računu Rekono, in enkratno varno geslo, ki ga prejme v SMS-sporočilu.

11. V primeru uporabe mobilne aplikacije Rekono OnePass mora uporabnik ob vsakem nakupu na spletnem prodajnem mestu, ki podpira uporabo storitve Mastercard Identity Check in Visa Secure, pred izvedbo nakupa z uporabo mobilne aplikacije Rekono OnePass potrditi izvršitev plačila na podlagi prejetega potisnega obvestila.

12. Uporabnik pri varnem spletnem nakupu vnese enkratno varno geslo ali potrdi potisno obvestilo samo, če se na zaslonu, ki zahteva vpis gesla ali potrditev, izpišejo pravi trgovec, pravi znesek in prave zadnje štiri (4) številke njegove plačilne kartice, kar je uporabnik dolžan preveriti. Odsotnost ali nepravilnost navedenih podatkov na zaslonu lahko pomeni, da gre za spletno stran, ki želi pridobiti identifikacijske podatke imetnika kartice z namenom njihove zlorabe, zato imetnik kartice v takem primeru ne sme vpisati enkratnega varnega gesla ali potrditi potisnega obvestila in mora takoj zapreti spletni brskalnik oz. aplikacijo Rekono OnePass.

13. Za varnost in zaupnost mobilne naprave, na katero uporabnik prejema enkratna varna gesla, ali v kateri ima nameščeno mobilno aplikacijo Rekono OnePass, je odgovoren izključno uporabnik, pri čemer jo je dolžan skrbno

hraniti, da tako prepreči njeno izgubo, krajo in/ali zlorabo (na primer z zaklepanjem ekrana z geslom, PIN-om ali vzorcem svojega prstnega odtisa).

14. Uporabnik je dolžan banko, ki mu je izdala plačilno kartico, in/ali družbo Rekono nemudoma obvestiti o izgubi, kraji in/ali zlorabi mobilne naprave in o kakršni koli nepooblaščeni uporabi enkratnih varnih gesel ali sumu, da je ali da bi njegov račun Rekono ali druge podatke in naprave za izvedbo storitve za varno potrjevanje spletnih nakupov v njegovem imenu lahko zlorabila druga oseba. Uporabnik se mora zavedati, da je odgovoren za izvedbo vseh plačil za varne spletne nakupe, ki so bili potrjeni z Rekono OnePass ali Rekono SMS OTP na podlagi prijave z njegovim računom Rekono, ne glede na to, ali je bil žrtev goljufije.

15. Družba Rekono uporabniku ne bo odgovorna za kakršno koli škodo, ki bi nastala kot posledica uporabnikove uporabe ali poskusa uporabe Rekono 3D Secure oziroma onemogočenega, spremenjenega ali prekinjenega delovanja Rekono 3D Secure.

16. Družba Rekono lahko na zahtevo banke, ki potrjevanje plačil za varne spletne nakupe imetnikom njenih plačilnih kartic zagotavlja z Rekono 3D Secure, kadarkoli prekine ali ukine zagotavljanje omenjene storitve.

17. Upravljavke osebnih podatkov uporabnikov, ki plačila za varne spletne nakupe potrjujejo z Rekono 3D Secure, so banke, in sicer vsaka za imetnike njenih plačilnih kartic. Družba Rekono ima z vsako od bank sklenjeno pogodbo o obdelavi podatkov uporabnikov storitve Rekono 3D Secure, skladno s Splošno uredbo o varstvu podatkov.

5. OBDELAVA PODATKOV IN VARSTVO PRAVIC UPORABNIKA

1. Družba Rekono upravlja evidenco uporabnikov računa Rekono, ki vsebuje naslednje podatke:

   a) osebno ime uporabnika,
   b) navedba postopka ugotovitve in potrditve istovetnosti uporabnika pri registraciji računa Rekono oz. sredstva e-identifikacije,
   c) vrsta in številka veljavnega uradnega identifikacijskega dokumenta uporabnika, opremljenega s fotografijo, ki je bil uporabljen,
   d) davčno številko uporabnika oziroma EMŠO ali drug identifikacijski znak uporabnika (npr. PIN), če je to potrebno za registracijo in nastavitev ravni zanesljivosti računa Rekono oz. sredstva e-identifikacije,
   e) enotno številko elektronske identifikacije (EŠEI),
   f) stalno prebivališče oziroma začasno prebivališče uporabnika, če je to potrebno za registracijo in nastavitev ravni zanesljivosti računa Rekono oz. sredstva e-identifikacije,
   g) telefonsko številko mobilnega telefona uporabnika, če je to potrebno za registracijo in nastavitev ravni zanesljivosti računa Rekono oz. sredstva e-identifikacije,
   h) naslov elektronske pošte uporabnika, če je to potrebno za registracijo in uporabo računa Rekono,
   i) o lokaciji uporabnika storitve Rekono OnePass;
   j) o statusu računa Rekono,
   k) o obdobju veljavnosti računa Rekono,
   l) o obdobju začasne razveljavitve računa Rekono,
   m) datum preklica računa Rekono.

2. V sistemu Rekono se o uporabniku obdelujejo različni nabori osebnih podatkov glede na raven zanesljivosti računa Rekono:
   a) raven »0«: naslov uporabnikove e-pošte in številka njegovega mobilnega telefona, na katerega sprejema sporočila SMS;
   b) raven »10«: podatki ravni »0« + ime in priimek, datum rojstva, davčna številka, EŠEI in naslov prebivališča, številka in datum veljavnosti uradnega identifikacijskega dokumenta;
   c) raven »20« in »30«: podatki ravni »10« + kvalificirano potrdilo.

3. Namen obdelave podatkov o uporabniku računa Rekono in o elementih avtentikacije, ki jih uporablja v okviru tega računa, je uporabniku zagotoviti

storitve elektronske identifikacije in avtentikacije na ravni, ki mu omogoča uporabo storitev zaupanja Rekono in elektronskih storitev ponudnikov, ki se na te storitve zanašajo.

4. Namen obdelave podatkov o lokaciji uporabnika storitve Rekono OnePass je preprečevanje zlorab. Podatki se hranijo kot dodatni atribut v dnevniških zapisih, uporablja pa jih sistem za detekcijo in preprečevanje zlorab.

5. Upravljavec lahko uporabnikove podatke iz računa Rekono–v obsegu, nujnem za izvedbo posameznega postopka identifikacije oz. avtentikacije ali storitve zaupanja, na zahtevo uporabnika posreduje ponudniku elektronske storitve, ki se na ta postopek oz. storitev zanaša.

6. Podatki posameznega računa Rekono se hranijo še deset let po koncu veljavnosti računa.

7. Avtomatizirano sprejemanje odločitev ali profiliranje se v okviru storitev Rekono ne izvaja.

8. Uporabnik ima v zvezi z obdelavo podatkov njegovega računa Rekono od upravljavca pravico zahtevati dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi z njim ter pravico do ugovora obdelavi in pravico do prenosljivosti podatkov. Zahteva posameznika se obravnava skladno z določbami Splošne uredbe. Naslov za uveljavljanje pravic v zvezi z obdelavo podatkov je info@rekono.si.

9. Na spletni strani Informacijskega pooblaščenca lahko uporabnik prek obrazca poda prijavo zaradi kršitev zakonodaje s področja varstva osebnih podatkov.

6. ODGOVORNA UPORABA TER ODPOVED ALI PREKLIC UPORABE RAČUNA REKONO

1. Da se prepreči zloraba računa Rekono, mora uporabnik elemente oz. postopke avtentikacije uporabljati oz. izvajati z vso potrebno skrbnostjo in odgovornostjo. Uporabnik je odgovoren za izbiro najustreznejšega elementa avtentifikacije glede na namen in način uporabe računa Rekono.

2. Uporabnik mora morebitne spremembe svojih registracijskih podatkov v računu Rekono nemudoma posodobiti.

3. Uporabnik mora zaradi preprečitve zlorabe svojega računa Rekono skrbno ravnati s podatki elementov za avtentikacijo za dostop do računa, da se ne razkrijejo drugim in da se prepreči možna zloraba teh podatkov oz. računa Rekono.

4. Uporabnik mora vsak sum zlorabe svojih podatkov oz. elementov avtentikacije za dostop do računa storitve Rekono nemudoma sporočiti upravljavcu po elektronski pošti na naslov info@rekono.si.

5. Uporabnik je odškodninsko odgovoren za vsakršno škodo, ki jo je povzročil s posredovanjem ali malomarno uporabo svojih podatkov za dostop in uporabo računa Rekono.

6. Uporabnik lahko uporabo računa Rekono kadar koli odpove s funkcijo »Ukinitev uporabniškega računa« v nadzorni plošči računa Rekono. Po odpovedi bodo uporabnikovi podatki v računu Rekono hranjeni in izbrisani v skladu s predpisi, ki urejajo elektronsko identifikacijo in storitve zaupanja ter varstvo osebnih podatkov.

7. Upravljavec lahko po večkratnem neuspešnem poskusu prijave z izbranim elementom avtentikacije onemogoči dostop do določenega računa Rekono.

8. Upravljavec lahko v primeru zlorabe računa Rekono uporabniku prekliče pravico uporabe računa s takojšnjim učinkom, uporabnikove podatke pa shrani v skladu s predpisi, ki urejajo elektronsko identifikacijo in storitve zaupanja ter varstvo osebnih podatkov.

9. Upravljavec ne prevzema nobene odškodninske ali druge odgovornosti za škodo in druge posledice, ki so nastale zaradi zlorabe računa Rekono s strani

uporabnika ali tretje osebe ali preklica pravice uporabe računa Rekono. Za zlorabo velja zlasti:

a) če da uporabnik svoje elemente avtentikacije oz. račun Rekono v uporabo drugemu posamezniku, da se ta v pravnih poslih lažno predstavlja z identiteto uporabnika,
b) če uporabnik z identiteto, avtenticirano preko računa Rekono, z neželenim oglaševanjem ali v kakšni drugačni obliki druge osebe nadleguje, jih ogroža ali jim škoduje,
c) če uporabnik z identiteto, izkazano in zatrjevano z računom Rekono, pri priklicu in shranjevanju, posredovanju, distribuciji ali prikazu določenih vsebin krši zakonske omejitve (na primer zakonodajo o avtorskih pravicah, prepovedi, osebnostne pravice po kazenskem in obligacijskem zakonu),
d) če uporabnik zaznane zlorabe svojih podatkov za uporabo računa Rekono ne opusti ali ne prepreči,
e) če uporabnik samostojno ali v sodelovanju z drugim avtentikacijo s svojim računom Rekono uporabi za nepooblaščeno analiziranje sistemskih funkcij storitev Rekono ali podatkov v napravah, podatkovnih zbirkah ali storitvah oziroma za manipuliranje s temi podatki in/ali dokumenti,
f) vsakršna zloraba, ki je posledica ali ima znake kaznivega dejanja s strani tretje osebe.

10. Račun Rekono se samodejno ukine v primeru neaktivne uporabe računa v obdobju 3 let.

7. VAROVANJE ZAUPNOSTI PODATKOV RAČUNA REKONO IDENTIFIKACIJSKIH SREDSTEV IN POSTOPKOV TER IN ZAGOTAVLJANJE REVIZIJSKIH SLEDI

1. Upravljavec podatke o uporabniku in ostale podatke, povezane z njegovim računom Rekono, varuje v skladu z zahtevami Splošne uredbe o varstvu podatkov, veljavnim zakonom o varstvu osebnih podatkov in notranjim aktom upravljavca o zagotavljanju varnosti obdelave osebnih podatkov. Upravljavec je imetnik certifikatov ISO 9001, ISO/IEC 27001 in ISO/IEC 20000-1.

2. Uporabnik mora varovati zaupnost podatkov računa Rekono, še posebej elementov in postopkov avtentikacije ter jih uporabljati v skladu s temi splošnimi pogoji in navodili za uporabo računa Rekono oz. posameznih elementov avtentikacije, če obstajajo. V primeru malomarnega ravnanja ali zlorabe računa Rekono, ki ima škodljive posledice za družbo Rekono ali druge uporabnike storitev Rekono, je uporabnik lahko odškodninsko ali kazensko odgovoren.

3. Uporabnik je dolžan še posebej skrbno varovati identifikacijsko kodo, ki izkazuje lastništvo računa Rekono (t.i. kodo PUK), in ki uporabniku omogoča dostop in ponastavitev njegovega računa Rekono, če je pozabil geslo oz. izgubil lastništvo nad ostalimi sredstvi e-identifikacije.

4. Vsi uporabnikovi postopki uporabe računa Rekono in dostopi drugih pooblaščenih oseb do podatkov računa Rekono (t.i. revizijske sledi) se beležijo v namenskem podatkovnem skladišču sistema Rekono, pri čemer je vsak zapis revizijske sledi podpisan z zasebnim ključem, shranjenim na varni strojni napravi. Shranjene revizijske sledi upravljavec uporablja le za obravnavanje uporabnikovih zahtevkov za varstvo njegovih pravic v zvezi z obdelavo podatkov o njem ter za statistične obdelave za namene izboljšanja storitev oz. delovanja sistema Rekono. Upravljavec na podlagi zakonitih zahtevkov zapis revizijske sledi lahko posreduje pristojnim državnim organom.

8. STROŠKI UPORABE RAČUNA REKONO

1. Registracija in uporaba računa Rekono ravni zanesljivosti »0« in »10« je za uporabnika brezplačna.

2. Stroški registracije in uporabe računa Rekono ravni zanesljivosti »20« in »30« so praviloma vezani na uporabo storitve zaupanja določenega ponudnika, ki določi način njihovega obračunavanja.

9. PRAVICE IN OBVEZNOSTI UPRAVLJAVCA

1. Upravljavec lahko v primeru zlorabe storitve Rekono uporabniku onemogoči uporabo njegovega računa Rekono s takojšnjim učinkom in nemudoma izvede druge potrebne varnostne ukrepe in postopke za omejitev posledic zlorabe.

2. Upravljavec se zavezuje, da bo uporabniku do odpovedi uporabe storitve Rekono ohranil razpoložljivost storitve Rekono ter da bo po zaključku uporabniškega razmerja njegove podatke v računu Rekono hranil in izbrisal v skladu z relevantnimi predpisi.

10. RAZPOLOŽLJIVOST STORITEV REKONO

1. Storitve Rekono so uporabniku na voljo 24 ur na dan in sedem dni v tednu. Ker je treba občasno izvajati servisna in vzdrževalna dela na sistemih, v tem obdobju Rekono morda začasno ne bo na voljo. Upravljavec izrecno opozarja, da začasne nezmožnosti uporabe storitev nikoli ni mogoče povsem izključiti. Upravljavec v zvezi s tem jamči samo za škodo, nastalo zaradi nedostopnosti storitev Rekono, povzročeno z grobo malomarnostjo ali naklepom. Odgovornost za posredno škodo ali izgubljeni dobiček je v celoti izključena.

2. Upravljavec ni odgovoren, če uporabnik do računa Rekono lahko dostopa samo omejeno ali sploh ne, če so razlogi za to na strani tehničnih komponent (npr. strojne in programske opreme) ali razpoložljivosti internetnega dostopa pri uporabniku.

11. PIŠKOTKI

1. Spletno mesto rekono.si uporablja piškotke, ki omogočajo nemoteno delovanje storitve. V uporabo piškotkov privolite z uporabo naših storitev. Več o piškotkih si preberite v Politiki zasebnosti spletne strani rekono.si[1].

[1] https://www.rekono.si/sl/politika-zasebnosti/

12. SPREMEMBE STORITEV REKONO IN SPLOŠNIH POGOJEV

1. Upravljavec lahko splošne pogoje občasno spremeni ali dopolni zaradi sprememb v vsebini ali načinu delovanja storitev Rekono, kadar to zahtevajo:

a) novi ali spremenjeni predpisi;
b) regulatorji ali spremembe tehničnih specifikacij oz. standardov; ali
c) ugotovljene potrebe po izboljšanju storitev ali načina delovanja sistema Rekono.

2. Če posodobitev vpliva na uporabo storitev ali zakonite pravice uporabnika računa Rekono, upravljavec uporabnike o tem obvesti vsaj 15 dni pred datumom začetka veljavnosti posodobitve tako, da pošlje e-poštna sporočila na e-poštne naslove, povezane z računi Rekono, in z objavo obvestila na spletni strani www.rekono.si. Če se posamezni uporabnik ne strinja s sporočenimi posodobitvami, lahko račun Rekono prekliče, preden spremembe začno veljati. Z uporabo storitev oz. dostopom do računa Rekono po uveljavitvi posodobitev uporabnik izrazi strinjanje z novimi splošnimi pogoji in s spremenjenim pogodbenim razmerjem z upravljavcem, vezanim na uporabo računa Rekono.

13. REŠEVANJE SPOROV

1. Uporabnik lahko vsa vprašanja, pritožbe ali zahtevke v zvezi z uporabo računa in storitev Rekono, kakor tudi v zvezi z varnostjo njegovih osebnih podatkov pri uporabi storitve Rekono, pošlje na info@rekono.si. Upravljavec si bo prizadeval za čimprejšnji odgovor, najkasneje v zakonsko določenih rokih.

2. Upravljavec si bo vse morebitne spore iz te pogodbe prizadeval reševati sporazumno, če pa to ne bo mogoče, bo spore reševalo stvarno pristojno sodišče v Ljubljani.

14. REFERENCE

(1) UREDBA (EU) št. 910/2014 EVROPSKEGA PARLAMENTA IN SVETA z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (Uredba eIDAS)

(2) IZVEDBENA UREDBA KOMISIJE (EU) 2015/1502 z dne 8. septembra 2015 o določitvi minimalnih tehničnih specifikacij in postopkov za ravni zanesljivosti za sredstva elektronske identifikacije v skladu s členom 8(3) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (IUK eID)

(3) Zakon o elektronskem poslovanju in elektronskem podpisu – ZEPEP (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14)

(4) Zakon o preprečevanju pranja denarja in financiranja terorizma ZPPDFT-2 (Uradni list RS, št. 47/2022)

(5) Zakon o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih - ZPlaSSIED (Uradni list RS, št. 7/18, 9/18 – popr. in 102/20)

(6) Zakon o elektronski identifikaciji in storitvah zaupanja – ZEISZ (Uradni list RS, št. 121/21 in 189/21 – ZDU-1M)

(7) DELEGIRANA UREDBA KOMISIJE (EU) 2018/389 z dne 27. novembra 2017 o dopolnitvi Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta glede regulativnih tehničnih standardov za močno avtentikacijo strank ter skupnih in varnih odprtih standardov komunikacije (RTS SCA)

(8) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)