Splošni pogoji uporabe storitve Rekono

Ljubljana, november 2020

Zaščita dokumenta

© podjetje Rekono d.o.o.
Vse pravice pridržane. Reprodukcija po delih ali v celoti na kakršenkoli način in v kateremkoli mediju ni dovoljena brez pisnega dovoljenja avtorja. Kršitve se sankcionirajo v skladu z avtorsko, pravno in kazensko zakonodajo.

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**

Nadzor različic dokumenta

Izvirni dokument je shranjen v elektronski obliki, različice dokumenta so pod nadzorom. Morebitne papirne ali elektronske kopija tega dokumenta lahko obstajajo za namene razdeljevanja tistim, ki jim je dokument namenjen oz. se morajo z njim seznaniti v okviru izvajanja delovnih nalog. Kopije dokumenta niso nadzorovane in jih mora bralec obravnavati kot take.

Zgodovina sprememb dokumenta:

Razl.	Status	Avtor	Datum	Opis / opomba
1.0	odobren	Marjan Antončič	1.5.2016	Verzija 1.0
2.0	odobren	Marjan Antončič	11.9.2019	Prilagoditev politik za bančne uporabnike
3.0	odobren	Miha Poberaj	1.4.2020	Dodani Rekono.TSP in Rekono OnePass
4.0	odobren	Miha Poberaj	16.11.2020	Dodani postopki identifikacije, mehanizmi za avtentikacijo in registracijska pisarna

Kazalo

1. SPLOŠNO

1. Ti splošni pogoji urejajo uporabo spletne storitve za elektronsko identifikacijo in avtentikacijo Rekono (v nadaljevanju: Rekono), ki jo uporabnikom zagotavlja podjetje Rekono d.o.o. (v nadaljevanju: »podjetje Rekono« oz. upravljavec). Uporabnik s sprejetjem splošnih pogojev in registracijo svoje pravne identitete z odprtjem računa v okviru storitev Rekono (v nadaljevanju: račun Rekono) pridobi pravico, da svoj račun Rekono z izbranim identifikacijskim sredstvom in avtentikacijskim postopkom uporablja v storitvah zaupanja za elektronske transakcije in drugih rešitvah oz. storitvah, vezanih na zanesljivo in varno predstavitev oz. potrditev (avtentikacijo) uporabnikove identitete.

2. Z registracijo in odprtjem računa Rekono uporabnik z upravljavcem 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 storitev Rekono.

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 dodatnim pogojem, ki jih določi ponudnik te storitve.

4. Politika Rekono.TSP in opisi delovanja storitev 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

1.1. 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 mobilni napravi in podjetje 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 sporočil in enkratnih kod (TOTP).
d) »SMS-OTP« je enkratno geslo, namenjeno prijavi v Rekono, s SMS poslano na mobilni telefon uporabnika.
e) »Uporabnik« je fizična oseba, ki 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;
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.

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).

1.2. 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	enkratne kode poslane 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 Rekono.si prijavi 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 registracijo računa Rekono, je odvisna od postopka registracije, načina dokazovanja in preverjanja uporabnikove identitete, lastnosti sredstva elektronske identifikacije, načina izdaje in aktivacije tega sredstva ter njegove uporabe. Našteti postopki so v sistemu Rekono izvedeni v skladu z Uredbo (EU) št. 910/2014 in na njeni podlagi izdani Izvedbeni uredbi Komisije (EU) 2015/1502 ter relevantnimi tehničnimi specifikacijami in standardi.

3. Rekono obsega izdajanje in upravljanje sredstev e-identifikacije 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 sistema Rekono so uporabniku na voljo sledeča identifikacijska sredstva:

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 spremenljive enkratne kode (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 – enkratne kode, poslane na mobilni telefon po SMS;
f) kvalificirano potrdilo – omogočena je registracija in uporaba kvalificiranih potrdil overiteljev, registriranih v Sloveniji.

5. Ob registraciji posameznega identifikacijskega sredstva Rekono vedno izvede potrditev lastništva oziroma posedovanja (proof-of-possession) identifikacijskega sredstva, izdanega določenemu uporabniku. Potrditev se izvede za vsa v prejšnji točki navedena sredstva, in sicer:
a) za potrditev posedovanja elektronskega poštnega naslova 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 močno avtentikacijo;
c) za potrditev posedovanja mobilnega telefona za SMS-OTP na številko mobilnega telefona, ki jo je v postopku registracije navedel uporabnik, Rekono pošlje enkratno kodo 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.

6. Identifikacijska sredstva sistema Rekono uporabniku omogočajo močno dvofaktorsko avtentikacijo. Za izkazovanje in zagotavljanje srednje ali visoke ravni zaupanja v njegovo 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.

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 bančne kartice, ki je bila izdana na podlagi oddaljene identifikacije, ali s
   c) potrditvijo svoje identitete preko oddaljene identifikacije preko registracijske pisarne Rekono.

10. Za visoko raven zaupanja mora uporabnik potrditi svojo identiteto
   a) preko registracijske pisarne Rekono s fizično identifikacijo, ali
   b) v svojem računu Rekono registrirati veljavno kvalificirano potrdilo, ki je bilo izdano na napravi za ustvarjanje kvalificiranega elektronskega podpisa ali
   c) izvesti registracijo z veljavno kombinacijo številke PAN in PIN svoje bančne kartice, ki je bila izdana na podlagi fizične identifikacije.

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.

12. Uporabniku avtentikacija z računom Rekono, ki zagotavlja visoko raven zaupanja v njegovo identiteto, omogoča ustvarjanje kvalificiranega elektronskega podpisa v sistemu za elektronski podpis na daljavo Subscribo.

4. OBDELAVA PODATKOV IN VARSTVO PRAVIC UPORABNIKA

1. V računu, ki ga v sistemu Rekono odpre uporabnik, se o uporabniku obdelujejo različni nabori osebnih podatkov glede na želeno raven zanesljivosti identifikacijskega sredstva 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 in naslov prebivališča, številka in datum veljavnosti osebnega identifikacijskega dokumenta;
   c) raven »20« in »30«: podatki ravni »10« + kvalificirano potrdilo

2. Namen obdelave podatkov o uporabniku storitev Rekono je zagotavljanje storitve elektronske identifikacije in avtentikacije za posameznike, ki so z upravljavcem sklenili pogodbo za uporabo storitev Rekono.

3. Osebni podatki uporabnikov storitev Rekono se hranijo trajno.

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

5. Uporabnik ima 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.

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

5. ODGOVORNA UPORABA TER ODPOVED ALI PREKLIC UPORABE RAČUNA REKONO

1. Da se prepreči zloraba identifikacijskih sredstev in avtentikacijskih postopkov računa Rekono, jih mora uporabnik uporabljati z vso potrebno skrbnostjo in odgovornostjo. Uporabnik je odgovoren za izbiro najustreznejšega identifikacijskega sredstva glede na namen in način uporabe računa Rekono.

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

3. Uporabnik mora zaradi preprečitve zlorabe njegovega računa Rekono skrbno ravnati s podatki 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 njegovih podatkov za dostop do računa storitve Rekono nemudoma sporočiti upravljavcu po elektronski pošti na naslov info@rekono.si, poleg tega pa mora povrniti vsakršno škodo, ki jo je povzročil s posredovanjem ali malomarno uporabo svojih podatkov za dostop.

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

6. Upravljavec lahko po večkratnem neuspešnem poskusu prijave z uporabniškim imenom in geslom uporabniku onemogoči dostop do računa Rekono.

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

8. Upravljavec ne prevzema nobene odškodninske ali druge odgovornosti za škodo in druge posledice, ki so nastale zaradi uporabnikove zlorabe računa Rekono ali preklica pravice uporabe računa Rekono. Za zlorabo velja zlasti:

a) če da uporabnik svoje identifikacijsko sredstvo 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, avtenticirano preko računa 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) ali zlorabe svojih podatkov za dostop ne opusti ali ne prepreči,
d) 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.

6. VAROVANJE ZAUPNOSTI IDENTIFIKACIJSKIH SREDSTEV IN POSTOPKOV TER 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 2000-1.

2. Uporabnik mora varovati zaupnost identifikacijskih sredstev in avtentikacijskih postopkov in jih uporabljati v skladu s temi splošnimi pogoji in navodili. V primeru malomarnega ravnanja ali zlorabe računa Rekono, ki ima škodljive posledice za podjetje 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 mehanizmi avtentikacije.

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.

7. STROŠKI UPORABE RAČUNA REKONA

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

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

8. PRAVICE IN OBVEZNOSTI UPRAVLJAVCA

1. Upravljavec lahko v primeru zlorabe storitve Rekono uporabniku onemogoči uporabo njegovega računa storitve 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.

9. 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, povzročene 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.

10. 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/

11. 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.

12. 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.

13. REFERENCE

[1] eIDAS "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"

[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

[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-1 (Uradni list RS, št. 68/16, 81/19 in 91/20)

[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)