|  |
| --- |
| **\\filee\home\kristelk\Desktop\RIA mallid\logo2_oige.png** |

**ANDMETÖÖTLUSLEPING**

1. **ÜLDSÄTTED**
   1. Käesolev andmetöötlusleping (edaspidi *ATL*) on sõlmitud […] (edaspidi ***vastutav töötleja***) ja Riigi Infosüsteemi Ameti (edaspidi ***volitatud töötleja***) vahel andmesubjektile tema isikuandmetele juurdepääsu võimaldamiseks Andmejälgija teenuse vahendusel (edaspidi *teenus*) teabevärav Eesti.ee portaali (edaspidi *Riigiportaal*) kaudu.
   2. Vastutav töötleja on esitanud volitatud töötlejale taotluse teenuse avamiseks Riigiportaalis ning on nõustunud taotluse esitamisel teenuse osutamise tingimustega.
   3. Volitatud töötleja töötleb seoses teenuse osutamisega isikuandmeid vastutava töötleja nimel.
   4. Isikuandmete töötlemisel kohustuvad pooled juhinduma kehtivatest õigusaktidest, sealhulgas avaliku teabe seadusest ning Euroopa Parlamendi ja nõukogu 27. aprill 2016. a määrusest (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) ja isikuandmete kaitse seadusest.
2. **POOLTE KOHUSTUSED**
   1. Vastutava töötleja kohustused
      1. Vastutav töötleja on kohustatud tagama, et teenuse kasutamisega seotud isikuandmete töötlemiseks on kohaldatava õiguse kohaselt õiguslik alus ja isikuandmete töötlemine toimub õigustatud eesmärkidel.
      2. Andmesubjekti päringule tema isikuandmete töötlemise kohta vastab Riigiportaali päringu teinud asutus või ettevõte.
   2. Volitatud töötleja kohustused
      1. Volitatud töötleja on kohustatud rakendama teenuse osutamisel isikuandmete turvalisuse tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid, hõlmates muu hulgas vastavalt vajadusele järgmist: isikuandmete pseudonümiseerimine ja krüpteerimine; võime tagada isikuandmeid töötlevate süsteemide ja teenuste kasutamisel kogutud isikuandmete kestev konfidentsiaalsus, terviklus, kättesaadavus ja vastupidavus; võime taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi korral; tehniliste ja korralduslike meetmete tõhususe korrapärase testimise ja hindamise kord isikuandmete töötlemise turvalisuse tagamiseks vastavalt Riigiportaali teenustaseme tingimustes toodule.
      2. Volitatud töötleja teeb kõik endast sõltuva, et kaitsta töödeldavaid isikuandmeid loata või ebaseadusliku töötlemise ning juhusliku kaotamise, hävitamise või avalikustamise eest.
      3. Kui volitatud töötleja kahtleb vastutava töötleja poolt määratud tehniliste ja korralduslike meetmete asjakohasuses ja piisavuses, teatab ta sellest viivitamatult vastutavale töötlejale.
      4. Volitatud töötleja tagab tehniliste ja korralduslike meetmete rakendamise valmisoleku enne isikuandmete töötlemisega alustamist.
      5. Volitatud töötlejal ei ole õigust töödelda teenuse osutamisel andmesubjekti isikuandmeid oma või mis tahes muudel eesmärkidel kui need, mis on sätestatud käesolevas ATL-is.
      6. Teenuse osutamisel aset leidnud isikuandmete töötlemise rikkumise korral teavitab volitatud töötleja sellest viivitamatult vastutavat töötlejat e-posti aadressil […]. Teates annab volitatud töötleja vastutavale töötlejale teavet asjaoludest, mis on põhjustanud isikuandmetega seotud rikkumise, ning ükskõik mis muust isikuandmete vastutava töötleja poolt mõistlikult nõutud seonduvast teabest, mis isikuandmete volitatud töötlejale kättesaadav on.
   3. Pool esitab teisele poolele käesoleva lepingu alusel toimuva isikuandmete töötlemise kohta kõik vajalikud andmed ja dokumendid, kui see on vajalik poolele kohaldatava õiguse kohaselt pandud ülesannete täitmiseks. Pool esitab teisele poolele kogu teabe ja dokumentatsiooni ning osutab vajalikku abi, et poolel oleks võimalik pidada kinni kohaldatava õiguse nõuetest ning tõendada vastavust sellistele nõuetele.
   4. Kui andmesubjekt taotleb poolelt teavet tema kohta kogutud isikuandmete kohta, teevad pooled andmesubjekti vastava taotluse lahendamisel koostööd ja abistavad teineteist koondamaks teavet asjakohaste tehniliste ja korralduslike meetmete kohta, mida pool isikuandmete töötlemise rakendab. Volitatud töötleja peab tagama, et tema süsteemid ja protsessid oleksid üles ehitatud nii, et punktis 2.1.2 märgitud andmetöötlejal oleks alati võimalik kõigi andmesubjektide taotlustele kiiresti vastata ning asjaomaste vastuste suhtes kohaldatava õigusega sätestatud tähtaegadest kinni pidada.
   5. Kui andmekaitse- või muu järelevalveasutus algatab vastutava töötleja poolt läbi viidud isikuandmete töötlemise toimingute läbivaatamise või kui andmesubjekt esitab vastutava töötleja kohta kaebuse ja see kaebus on seotud volitatud töötleja poolt läbi viidud isikuandmete töötlemisega, abistab volitatud töötleja vastutavat töötlejat dokumentide ja teabe avaldamisel asjaomastele pädevatele asutustele.
3. **RIKKUMINE JA VASTUTUS**
   1. Pool vastutab teisele poolele käesoleva ATL-i või kohaldatava õiguse või pädeva andmekaitseasutuse otsusega vastuolus oleva tegevusega tekitatud kahju eest.
   2. Kui poole vastu suunatud nõue või trahv on põhjustatud käesoleva ATL-i või kohaldatava õiguse rikkumisest, teavitab rikkunud poolt teist poolt sellest viivitamatult ning rakendab kõikvõimalikke meetmeid, et leevendada sellisest rikkumisest tulenevat kahju.
4. **KONTAKTISIKUD**
   1. Volitatud töötleja kontaktandmed:
      1. Andmejälgija tootejuht

|  |  |
| --- | --- |
| Nimi: | Piret Pärna |
| E-post: | piret.parna@ria.ee |
| Telefon: | +372 5830 3759 |

* + 1. Riigi Infosüsteemi Ameti andmekaitsespetsialist

|  |  |
| --- | --- |
| Nimi: | Mehis Lõhmus |
| E-post: | andmekaitse@ria.ee |
| Telefon: | +372 5553 0290 |

* 1. Vastutava töötleja kontaktandmed:

|  |  |
| --- | --- |
| Nimi: |  |
| E-post: |  |
| Telefon: | +372 |

1. LEPINGU KESTUS
   1. Käesolev ATL kehtib teenuse osutamisel tähtajatult.
2. **LEPINGU LÕPPEMINE JA ANDMETE TAGASTAMINE/KUSTUTAMINE**
   1. Teenuse osutamise lõpetamisel lõpeb volitatud töötleja õigus töödelda käesoleva ATL-i alusel vastutava töötleja nimel andmesubjekti isikuandmeid automaatselt.
   2. ATL-i lõppemisel kustutab volitatud töötleja kõik teenuse osutamisel kogutud isikuandmed ning esitab vastutavale töötlejale tema poolt nõutud andmed ja teabe. Pooltel on õigus sõlmida täiendavaid kokkuleppeid isikuandmete töötlemise lõpetamise tingimustes.
3. **KOHALDATAV ÕIGUS**
   1. Käesolevale ATL-ile kohaldatakse Eesti Vabariigis kehtivat õigust.
   2. Käesolevast ATL-st tulenevad vaidlused lahendatakse poolte vahel läbirääkimiste teel. Kui pooled kokkulepet ei saavuta, lahendatakse vaidlus vastavalt Eesti Vabariigis kehtivatele seadustele.
4. **LISAD**

LISA nr. 1 – ISIKUANDMETE KIRJELDUS

|  |  |  |
| --- | --- | --- |
| **Asutuse nimi** |  | **Riigi Infosüsteemi Amet** |
| */allkirjastatud digitaalselt/* |  | */allkirjastatud digitaalselt/* |
| Esindaja nimi |  | Margus Noormaa |
| Ametikoht |  | Peadirektor |

**LISA nr. 1 – ISIKUANDMETE KIRJELDUS**

1. **Töötlemise objekt, laad ja eesmärgid**
   1. Töötlemise objekt on Riigi Infosüsteemi Ameti poolt […kellele?...] osutatav isikuandmete töötluse jälgimise teenus (Andmejälgija) läbi selleks loodud X-tee teenuse. Teenust osutatakse üle andmevahetuskihi X-tee ning selle kaudu on andmesubjektil võimalik teostada päringuid enda isikuandmete töötlemise kohta.
   2. Volitatud töötleja töötleb isikuandmeid vastutava töötleja nimel järgmistel eesmärkidel:

Teenus võimaldab volitatud töötlejal teha päring ning parsida tulemusi inimesele loetavale kujule - andmejälgija päring eesmärgiga kuvada inimesele tema isikuandmete töötluse logi, mille sisendiks on isikukood. Volitatud töötlejal ei ole õigust saadud andmeid eraldi talletada/salvestada.

1. **Töödeldavate isikuandmete liik ja kategooriad**

[…]

1. **Volitatud töötleja tehnilised ja korralduslikud turvameetmed**
   1. **Tehnilised turvameetmed**
      1. **TARA autentimine** isikustatud päringute tegemisel, alternatiivseid autentimisviise ei kasutata;
      2. Aktiivsete sessioonide info töötlemine **JSON Web Tokenite (JWT)** kujul, mis on laialtlevinud ja tehnoloogiliselt turvaline lahendus;
      3. **Riigiportaali komponent Ruuter** kui *backend-*i päringute orkestraator koostab ettenähtud äriloogika saavutamiseks vajalikud päringud teiste *backend-*i komponentide poole. Teenuste äriloogika on kirjeldatud rangelt struktureeritud konfiguratsioonifailides, mis tagab täiendava turvalisuse nii tehnilisel kui arhitektuursel tasemel (turvatestitud). Ruuteri funktsionaalsust kasutamata ei ole võimalik riigiportaalis teenuseid pakkuda, st Ruuterist ei ole võimalik mööda minna.
      4. Ruuter saadab esimese asjana **komponendile** **Turvis** kõik kasutaja poolt manipuleeritavad päringud (nt päringu perioodi algus- ja lõppkuupäeva muutmine), mida valideeritakse Turvise vastavate teenuste kontrollide vastu (kirjeldatud eraldi konfiguratsioonifailidena). Kui päringu sisendis tuvastatakse vähimgi kõrvalekalle lubatud struktuurist (sisendite *whitelist*-imine), siis kogu edasine tegevus peatatakse ja isikustatud päringute tegemiseni ei jõuta.
      5. X-tee päringuid teostab **komponent XTR**, mille poole saab päringuid teha vaid komponent Ruuter.
      6. X-tee päringute vastused viib frontendi jaoks loetavale kujule **komponent Andmemuundur**, mille poole saab päringuid teha vaid komponent Ruuter.
      7. Kõikide komponentide ehitamisel loetakse tundlikud parameetrid sisse **Vault muutujatena.** See tähendab, et tundlikud andmed, mis võimaldaksid süsteemi kompromiteerida, ei leki arendaja hooletusest näiteks koodirepositooriumite kaudu.
      8. Komponentide-vaheline liiklus
         1. toimub üle **TLS 1.3;**
         2. on täiendavalt piiratud IP-põhiselt **„nftables“** abil.
      9. Kõikide komponentide logid talletatakse keskselt RIA logihoidlas.
      10. Kõik komponentide-vahelised päringud on seotud **Ruuteri poolt genereeritud Request ID** alusel, mis võimaldab iga päringu nii reaalajas kui tagantjärgi siduda algusest lõpuni ühtseks tervikuks.
      11. Kõik muudatused, sealhulgas teenuste Ruuteri konfiguratsioonide omad, tehakse läbi Giti, millega tagatakse nõuetekohane versioonihaldus.
      12. Arendajatel on ligipääs vaid arenduskeskkonnale, kus ei ole võimalik teha päringuid toodangukeskkonna X-tee (ega teiste teenuste toodangukeskkondade) vastu.
   2. **Korralduslikud turvameetmed**
      1. Ligipääs otse rakendusserveritesse üle SSH, logidele jt tundlikele andmetele toimub lähtuvalt RIA üldistest ligipääsupiirangute õiguste haldamisest. Ligipääsu toodangukeskkonna serveritele, logidele jm omavad vaid selleks volitatud isikud.