

Riigi Infosüsteemi Ameti autentimisteenuste andmekaitsetingimused

1. Käesolevas dokumendis selgitatakse, milliseid isikuandmeid ja mis eesmärgil Riigi Infosüsteemi Ameti (*edaspidi RIA*) autentimisteenustes töödeldakse.
2. Käesolevad andmekaitsetingimused rakenduvad:
 - Riigi autentimisteenusele (TARA)
 - Eesti autentimisteenusele (IdP)
 - RIA eIDAS konnektorteenusele
 - Euroopa Liidu piiriülese autentimistaristu Eesti sõlmele (“eIDAS Node”).
3. **Andmesubjekt** (*edaspidi kasutaja*) on füüsiline isik, kes suunatakse Eesti või välismaa klientrakendusest (nt e-teenusest) RIA autentimisteenusesse isikusamasuse tuvastamisele (autentimisele).

4. Autentimisandmed

- 4.1. Teenustes töödeldakse kasutajate kohta järgmisi andmeid (“autentimisandmed”):

Kasutajat identifitseerivad andmed:

- kasutaja isikukood vm isiku identifikaator;
- kasutaja ees- ja perekonnanimi;
- kasutaja sünniaeg;
- kasutaja riik;

Autentimistoimingu andmed:

- kuupäev ja kellaaeg;
- klientrakendus, kust kasutaja autentimisele suunati;
- autentimismeetod, sh pangalingi puhul ka pank; mobiil-ID puhul mobiilinumbrist;
- autentimise tulemus (autenditud või mitte).

4.2. Autentimisandmete väljastamine

- 4.2.1. Autentimisandmeid väljastatakse RIA autentimisteenusega liidestatud klientrakendusele või EL piiriülese autentimistaristu teise liikmesriigi sõlmele.
- 4.2.2. Andmete väljastamisel lähtutakse isikuandmete töötlemise minimaalsuse põhimõttest. Väljastatakse minimaalsed autentimise fakti ja tuvastatud isikut identifitseerivad andmed. Näiteks mobiil-ID-ga autentimisel ei väljastata kasutaja mobiilinumbrist.
- 4.2.3. Kasutajale on autentimise tulemus (sisse logitud või mitte) nähtav sirvikus.
- 4.2.4. Eesti eID kasutaja autentimisandmete saatmisel Euroopa Liidu piiriülese autentimistaristuga liitunud teise riiki küsitakse kasutaja nõusolekut (Eesti autentimisteenuses).

5. Turvalogi

- 5.1. Teenuses logitakse autentimistoimingu andmed koos isikut identifitseerivate andmetega järgmistel eesmärkidel:

- 5.1.1. teenuse väärkasutamise, sh identiteedivarguste ja nende katsete, samuti küberrünnakute avastamiseks ja uurimiseks;
- 5.1.2. tehniliste tõrgete avastamiseks ja kõrvaldamiseks. Tehniline tõrge võib olla nii riist- kui ka tarkvara viga, võrguühenduse viga jms;
- 5.1.3. teenustega liidestatud e-teenuste omanike s.t asutuste poolt raporteeritud tehniliste probleemide põhjuste väljaselgitamiseks;
- 5.1.4. kasutajate pöördumiste (teated võimalike turvaprobleemide või tehniliste rikete kohta) menetlemiseks.
- 5.2. Logile juurdepääs on rangelt vajaduspõhine. Ligi pääsevad ainult teenuse käitamisega otseselt seotud süsteemi- ja teenusehaldurid, vajadusel ka turvainsidentide uurimisega tegelevad ametiisikud.
- 5.3. Logisid säilitatakse üks aasta.
- 5.4. Autentimisi soovitame logida ka klientrakenduse poolel. See on vajalik nii tehniliste tõrgete kui ka teenuse väärkasutuse tuvastamisel ja uurimisel.

6. Statistikalogi

- 6.1. Statistikalogi eesmärk on teenuste kasutamise kohta statistika tootmine teenuse juhtimise ja edasiarendamise eesmärgil.
- 6.2. Statistikalogisse kogutakse andmed autentimistoimingute kohta ilma isikut identifitseerivate andmeteta.
- 6.3. Statistikalogi põhjal koostatakse ja avalikustatakse isikuandmeid mittesisaldavaid statistilisi aruandeid.

7. Liidestatud asutuse kontaktisikud

Teenuste haldamise eesmärgil kogutakse liidestatud asutuste kontaktisikute andmeid.

8. Andmete väljastamine seaduse alusel

Andmeid võidakse väljastada ka juhul, kui seda näeb ette seadus (näiteks õiguskaitseasutusele kriminaalmenetluses või andmesubjektile tema taotlusel).