

## 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)
- Riigi SSO teenusele (GOVSSO)
- Euroopa Liidu piiriülese autentimistaristu Eesti sõlmele (Riiklik eIDAS-Node).

2.1 Käesolevad andmekaitsetingimused täiendavad ülaltoodud teenuste üldtingimusi.

3. **Andmesubjekt** (*edaspidi kasutaja*) on füüsiline isik, kes suunatakse Eesti või välisriigi klientrakendusest (nt e-teenusest) RIA autentimisteenustesse isikusamasuse tuvastamisele (autentimisele).

### 4. Isikuandmete töötlemise õiguslik alus

RIA töötleb isikuandmeid käesoleva dokumendi punktis 2 toodud teenuste raames seadusest ja RIA põhimäärusest tuleneva haldusülesandena, mis võimaldab isiku autentimist teenustega liitunud kliendi jaoks.

### 5. Autentimisandmed

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

Kasutajat identifitseerivad andmed:

- kasutaja autentimissertifikaat;<sup>1</sup>
- kasutaja isikukood vm isiku identifikaator;
- kasutaja ees- ja perekonnanimi;
- kasutaja sünniaeg;
- kasutaja riik;
- registrikood vm juriidilise isiku identifikaator;
- juriidilise isiku ärinimi;
- liidestunud e-teenuse kontaktisiku nimi, isikukood, e-posti aadress ja telefoni number.

Autentimistoimingu andmed:

- kuupäev ja kellaaeg;
- klientrakendus, kust kasutaja autentimisele suunati;
- autentimismeetod, sh mobiil-ID puhul mobiilinumbr;
- IP-aadress, millelt kasutaja autentimisele suunati;
- autentimise tulemus (autenditud või mitte).

---

<sup>1</sup> Sertifikaatide profiili kirjeldus on leitav: <https://www.skidsolutions.eu/repositoorium/profiil/>

## 5.2. Autentimisandmete väljastamine

- 5.2.1. Autentimisandmeid väljastatakse RIA autentimisteenustega liidestatud klientrakendusele või Euroopa Liidu piiriülese autentimistaristu teise liikmesriigi sõlmele (eIDAS-Node).
  - 5.2.1.1. ID-kaardi, mobiil-ID ja Smart-ID-ga autentimise korral saadetakse autentimisandmed SK ID Solutions AS-i välistele teenustele järgmises koosseisus:
    - 5.2.1.1.1. Kehtivuskinnitusteenus (kasutaja autentimissertifikaadi seerianumber);
    - 5.2.1.1.2. MID REST API veebiteenus (kasutaja isikukood ja mobiilinumbr);
    - 5.2.1.1.3. Smart-ID veebiteenus (kasutaja isikukood).
  - 5.2.2. Andmete väljastamisel lähtutakse isikuandmete töötlemise minimaalsuse põhimõttest. Väljastatakse minimaalsed autentimise fakti ja tuvastatud isikut identifitseerivad andmed. Näiteks mobiil-ID-ga autentimisel ei väljastata kasutaja mobiilinumbrit RIA autentimisteenustega liidestatud klientrakendustele ega Euroopa Liidu piiriülese autentimistaristu teise liikmesriigi sõlmele.
  - 5.2.3. Kasutajale on autentimise tulemus (sisse logitud või mitte) nähtav veebisirvikus.
- 5.3. Klientrakendustega suhtlemisel kasutatakse krüpteeritud kanaleid.
- 5.4. Eesti eID kasutaja autentimisandmete saatmisel Euroopa Liidu piiriülese autentimistaristuga (eIDAS-Node) liitunud teise riiki küsitakse TARAs kasutaja nõusolekut.

## 6. Turvalogi

- 6.1. Teenuses logitakse autentimistoimingu andmed koos isikut identifitseerivate andmetega järgmistel eesmärkidel:
  - 6.1.1. teenuse väärkasutamise, sh identiteedivarguste ja nende katsete, samuti küberrünnakute avastamiseks ja uurimiseks;
  - 6.1.2. tehniliste tõrgete avastamiseks ja kõrvaldamiseks. Tehniline tõrge võib olla nii riist- kui ka tarkvara viga, võrguühenduse viga vms;
  - 6.1.3. teenustega liidestatud e-teenuste omanike (asutuste) poolt raporteeritud tehniliste probleemide põhjuste väljaselgitamiseks;
  - 6.1.4. kasutajate pöördumiste (teated võimalike turvaprobleemide või tehniliste rikete kohta) menetlemiseks.
- 6.2. Logile juurdepääs on rangelt vajaduspõhine. Ligi pääsevad ainult teenuse käitamisega otseselt seotud süsteemi- ja teenusehaldurid, vajadusel ka turvaintsidentide uurimisega tegelevad ametiisikud.
- 6.3. Autentimisi soovitame logida ka klientrakenduse poolel. See on vajalik nii tehniliste tõrgete kui ka teenuse väärkasutuse tuvastamisel ja uurimisel.

## 7. Statistikalogi

- 7.1. Statistikalogi eesmärk on teenuste kasutamise kohta statistika tootmine teenuse juhtimise ja edasiarendamise eesmärgil.
- 7.2. Statistikalogisse kogutakse andmed autentimistoimingute kohta ilma isikut identifitseerivate andmeteta.
- 7.3. Statistikalogi põhjal koostatakse ja avalikustatakse isikuandmeid mittesisaldavaid statistilisi aruandeid.
- 7.4. Logisid säilitatakse üks aasta.

## 8. Liidestatud asutuse kontaktisikud

Teenuste haldamise eesmärgil kogutakse liidestatud asutuste kontaktisikute andmeid:

- kontaktisiku nimi;
- kontaktisiku e-posti aadress;
- kontaktisiku telefon;
- kontaktisiku isikukood.

## 9. Andmete varundamine

- 9.1 Varundusprotsess käivitatakse vähemalt korra ööpäeva jooksul. Kõikide teenuste komponentide andmete (konfiguratsioon, andmebaas, logid) tagavarakoopiaid säilitatakse ühe põhimõtte alusel – 7 päeva / 4 nädalat / 12 kuud.
- 9.2 Taastada on võimalik jooksva nädala päevade, jooksva kuu nädalate lõpu või viimase 12 kuu lõpu seisuga salvestatud andmed.
- 9.3 Varunduslahenduses krüpteerimist ei kasutata.

## 10. Turvalogide väljastamine

Turvalogi väljastatakse juhul, kui seda näeb ette seadus (näiteks õiguskaitseasutusele kriminaalmenetluses või andmesubjektile tema taotlusel).

## 11. Andmesubjekti õigused isikuandmete töötlemisel

- 11.1. Andmesubjektil on igal ajal õigus pöörduda RIA poole vastavasisulise lihtkirjaliku ja vabas vormis taotlusega e-posti aadressil [andmekaitse@ria.ee](mailto:andmekaitse@ria.ee), et:
  - 11.1.1. Taotleda juurdepääsu andmesubjekti kohta käivatele isikuandmetele;
  - 11.1.2. Asjakohasel juhul rakendada isikuandmete kaitse üldmääruse III peatükist tulenevaid muid õigusi.