KINNITATUD
Riigi Infosüsteemi Ameti peadirektori
11.02.2025 käskkirjaga nr 1.1-2/25-010

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:

2.1. Riigi autentimisteenusele (TARA);
2.2. Riigi SSO teenusele (GovSSO);
2.3. Euroopa Liidu piiriülese autentimistaristu Eesti sõlmele (Riiklik eIDAS-Node).

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. RIA autentimisteenustes töödeldakse kasutajate kohta järgmisi andmeid ("autentimisandmed"):
5.1.1. Kasutajat identifitseerivad andmed:
5.1.1.1. kasutaja autentimissertifikaat[1];
5.1.1.2. kasutaja isikukood vm isiku identifikaator;
5.1.1.3. kasutaja ees- ja perekonnanimi;
5.1.1.4. kasutaja sünniaeg;
5.1.1.5. kasutaja riik;
5.1.1.6. mobiiltelefoninumber;
5.1.1.7. kasutaja esindatavaid identifitseerivad andmed: füüsilise isiku ees- ja perekonnanimi ja isikukood vm isiku identifikaator ja riik, juriidilise isiku ärinimi ja registrikood ja riik;
5.1.1.8. volitustega antud esindusõiguse andmed;
5.1.1.9. kasutaja keelevalik;
5.1.1.10. Web eID veebisirvikulaienduse versioon ja omarakenduse versioon;
5.1.1.11. User-Agent HTTP päis ehk kasutaja veebisirvikut ja seadet profileeriv info.

5.1.2. Autentimistoimingu andmed:
5.1.2.1. kuupäev ja kellaaeg;
5.1.2.2. klientrakendus, kust kasutaja autentimisele suunati;
5.1.2.3. autentimismeetod (idcard/mobileid/smartid/eidas);

---

[1] Sertifikaatide profiili kirjeldus on leitav: https://www.skidsolutions.eu/repositoorium/profiil/

5.1.2.4. IP-aadress, millelt kasutaja autentimisele suunati;
5.1.2.5. autentimise tulemus (autenditud või mitte);
5.1.2.6. autentimisvahendi tase (high/substantial/low).

5.2. Autentimisandmete väljastamine
5.2.1. Autentimisandmed väljastatakse RIA autentimisteenustega liidestatud klientrakendustele ja Euroopa Liidu piiriülese autentimistaristu teise liikmesriigi sõlmele (eIDAS-Node) v.a punktides 5.1.1.1, 5.1.1.9, 5.1.1.10, 5.1.1.11 ja 5.1.2.4 nimetatud andmed.
5.2.2. ID-kaardi, Mobiil-ID ja Smart-ID-ga autentimise korral edastatakse autentimisandmed SK ID Solutions AS-i välistele teenustele järgmises koosseisus:
5.2.2.1. Kehtivuskinnitusteenus (kasutaja autentimissertifikaadi seerianumber);
5.2.2.2. Mobiil-ID teenus (kasutaja isikukood ja mobiiltelefoninumber);
5.2.2.3. Smart-ID teenus (kasutaja isikukood).
5.2.3. Esindatava valiku puhul edastatakse X-tee kaudu Äriregistri ja Pääsukese teenustele järgmised autentimisandmed: kasutaja riik ja isikukood.
5.2.4. Autentimisandmed võivad läbida ka veebiteenuste kaitseteenuse raames kolmanda osapoole teenuseid, kuid vaid piiratud osas, mis võimaldab eristada pahaloomulisi päringuid.
5.2.5. Andmete väljastamisel lähtutakse isikuandmete töötlemise minimaalsuse põhimõttest. Väljastatakse minimaalsed autentimise fakti ja tuvastatud isikut identifitseerivad andmed.
5.2.6. Kasutajale on autentimise tulemus (sisse logitud või mitte) nähtav veebisirvikus.
5.3. Klientrakenduste ja kõikide väliste osapoolte vahel, nt Euroopa Liidu autentimistaristu teise liikmesriigi sõlme (eIDAS-Node), SK ID Solutions AS-i teenustega (v.a kehtivuskinnitusteenus) 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. RIA autentimisteenustes logitakse punktis 5.1 nimetatud andmeid järgmistel eesmärkidel:
6.1.1. teenuste 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. RIA autentimisteenustega liidestatud e-teenuse 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 RIA autentimisteenuste 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.
6.4. Logisid säilitatakse 18 kuud.

7. Statistikalogi

7.1. Statistikalogi eesmärk on RIA autentimisteenuste kasutamise kohta statistika tootmine teenuste juhtimise ja edasiarendamise eesmärgil.
7.2. Statistikalogisse kogutakse punktides 5.1.2, 5.1.1.2, 5.1.1.5 ja 5.1.1.7 nimetatud andmed.
7.3. Statistikalogi põhjal koostatakse ja avalikustatakse isikuandmeid mittesisaldavaid statistilisi aruandeid.
7.4. Logisid säilitatakse 24 kuud.

8. Kontaktisikud

8.1. Parema klienditeeninduse tagamise eesmärgil kogutakse autentimisteenustega liidestatud klientrakenduse kontaktisikute andmeid:
8.1.1. kontaktisiku nimi;
8.1.2. kontaktisiku isikukood;
8.1.3. kontaktisiku e-posti aadress;
8.1.4. kontaktisiku telefon.

9. Küpsiste kasutamise poliitika

9.1. Küpsiste kasutamise poliitika (edaspidi *poliitika*) kirjeldab, milliseid küpsiseid RIA autentimisteenustes kasutatakse, millist teavet küpsiste abil kogutakse ja kuidas seda teavet kasutatakse.
9.2. RIA autentimisteenustes talletatakse veebisirviku poolel autentimisteenuste toimimiseks vajalikke isikuandmeid mittesisaldavaid küpsiseid:

Küpsise nimi	Aegumise tähtaeg	Eesmärk
__Host-LOCALE	1 aasta	Kasutaja keelevaliku salvestamiseks.
__Host-SESSION	Veebisirviku seanss	Unikaalse seansiidentifikaatori salvestamiseks.
JSESSIONID	Veebisirviku seanss	Unikaalse seansiidentifikaatori salvestamiseks.
JSESSIONID	15 minutit	Unikaalse seansiidentifikaatori salvestamiseks.
__Host-ory_hydra _session	Veebisirviku seanss	Unikaalse seansiidentifikaatori salvestamiseks.
__Host-ory_hydra_login _csrf_#	1 tund	# - unikaalne arv. Võltspäringuründe kaitseks unikaalse identifikaatori salvestamiseks.
__Host-ory_hydra_consent _csrf_#	1 tund	# - unikaalne arv. Võltspäringuründe kaitseks unikaalse identifikaatori salvestamiseks.
__Host-XSRF-TOKEN	1 tund	Võltspäringuründe kaitseks unikaalse identifikaatori salvestamiseks.

__Host-AUTH	1 tund	Võltspäringuründe ja taasesitusründe kaitseks unikaalsete identifikaatorite ja autentimistoimingu unikaalse identifikaatori salvestamiseks.

9.3. Veebiteenuste kaitseteenuse poolt defineeritud küpsised, mille nimed, tähtajad ja eesmärgid on kirjeldatud https://developers.cloudflare.com/fundamentals/reference/policies-compliances/cloudflare-cookies/.

9.4. Lisaks salvestatakse viimati kasutatud autentimisvahendi tüüp veebisirviku kohalikus andmehoidlas active-tab väärtuses.

9.5. RIA jätab endale õiguse vajaduse korral muuta autentimisteenustega seotud küpsiste poliitikat, kusjuures muudatused jõustuvad selle poliitika uuendatud versiooni avalikustamisel RIA kodulehel.

10. Andmete varundamine

10.1. Varundusprotsess käivitatakse vähemalt korra ööpäeva jooksul. Kõikide teenuste komponentide andmete (konfiguratsioon, andmebaas, logid) tagavarakoopiad säilitatakse ühe põhimõtte alusel – 7 päeva / 4 nädalat / 12 kuud.

10.2. Taastada on võimalik jooksva nädala päevade, jooksva kuu nädalate lõpu või viimase 12 kuu lõpu seisuga salvestatud andmed.

10.3. Varunduslahenduses krüpteerimist ei kasutata.

11. Turvalogide väljastamine

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

12. Andmesubjekti õigused isikuandmete töötlemisel

12.1. Andmesubjektil on igal ajal õigus pöörduda RIA poole vastavasisulise lihtkirjaliku ja vabas vormis taotlusega e-posti aadressil andmekaitse@ria.ee, et:

12.1.1. Taotleda juurdepääsu andmesubjekti kohta käivatele isikuandmetele;

12.1.2. Asjakohasel juhul rakendada isikuandmete kaitse üldmääruse III peatükist tulenevaid muid õigusi.