

Eesti Interneti SA juhatuse poolt heaks kiidetud 22.05.2026...

## Lisa 2

# Andmekaitsetingimused

## 1. Üldsätted

1.1 Käesolevad andmekaitsetingimused kohalduvad Eesti Interneti SA (edaspidi EIS) eeID elektroonilise identifitseerimisteenuse kasutamisel Kliendi ja EISi vahelises õigussuhtes ning täpsustavad Poolte õigusi ja kohustusi seoses isikuandmete töötlemisega.

1.2 Käesolevas dokumendis selgitatakse, milliseid isikuandmeid, mis eesmärkidel ja millistel õiguslikel alustel EIS eeID teenuse osutamisel töötleb ning kuidas jagunevad Poolte rollid isikuandmete töötlemisel.

1.3 Käesolevad andmekaitsetingimused reguleerivad eelkõige Kliendi ja EISi vahelisi suhteid ning neid tuleb tõlgendada koos Lepingu, teenuse tingimuste ja muude kohaldatavate õigusaktidega.

1.4 Füüsilistele isikutele suunatud teave eeID teenusega seotud isikuandmete töötlemise kohta on kirjeldatud eraldi dokumendis „eeID isikuandmete töötlemise põhimõtted andmesubjektile“ (Lisa 4).

## 2. Töödeldavad isikuandmed

2.1. Teenuse raames töödeldakse järgmisi isikuandmeid:

2.1.1. Kasutajat identifitseerivad andmed

- isikukood või muu identifikaator;
- registrikood vm juriidilise isiku identifikaator;
- ees- ja perekonnanimi;
- sünniaeg;
- riik;
- autentimissertifikaadi andmed.

2.1.2. Autentimis- ja tuvastustoimingu andmed

- kuupäev ja kellaeg;
- kliendirakendus (sh kust kasutaja autentimisele suunati);
- autentimismeetod, nt pangalingi puhul pank; mobiil-ID puhul mobiilnumber, ID-kaart, Smart-ID, videotuvastuse puhul video;
- autentimise või tuvastamise tulemus.

2.1.3. Kontaktandmed (vajadusel)

- liidestunud kliendi kontaktisiku nimi, isikukood, e-posti aadress ja telefoninumber

2.2. Autentimisandmete väljastamine

Eesti Interneti SA

Paldiski mnt 80, 10617 Tallinn, Estonia T +372 727 1000 E info@internet.ee www.internet.ee  
Reg. nr 90010019 VAT EE101286464

2.2.1. Autentimisandmeid väljastatakse EISi autentimisteenusega liidestatud kliendirakendusele.

2.2.2 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 EISi autentimisteenustega liidestatud kliendirakendusele.

2.2.3. Kasutajale on autentimise tulemus (sisse logitud või mitte) nähtav sirvikus.

2.2.4. Kliendirakendusega suhtlemisel kasutatakse krüpteeritud kanaleid.

### **3. Isikuandmete töötlemise eesmärgid, õiguslik alus ja edastamine**

3.1 Isikuandmeid töödeldakse järgmistel eesmärkidel:

- kasutaja isikusamasuse tuvastamine ja kinnitamine;
- turvalise elektroonilise identifitseerimise võimaldamine;
- teenuse toimimise tagamine;
- pettuste, väärkasutuse ja identiteedivarguste ennetamine, uurimine ja lahendamine;
- tehniliste tõrgete avastamine ja kõrvaldamine;
- turvaintsidentide uurimine.

3.2 Isikuandmete töötlemine toimub:

- lepingu täitmiseks (teenuse osutamine);
- õigustatud huvi alusel (turvalisus, pettuste ennetamine, uurimine ja lahendamine, süsteemi töökindlus);
- vajadusel õigusliku kohustuse täitmiseks.

3.3 Isikuandmeid edastatakse Kliendile minimaalsuse põhimõttel. Teenuse osutamisel võib isikuandmeid edastada kolmandatele teenusepakkujatele üksnes teenuse osutamiseks vajalikus ulatuses.

### **4. Kolmandad osapooled**

4.1. Teenuse osutamisel võib EIS kasutada kolmandaid teenusepakkujaid, sealhulgas autentimis-, isikutuvastus- ja muid tehnilisi teenusepakkujaid.

4.2. Kolmandad teenusepakkujad võivad sõltuvalt konkreetsest teenusest või töötlemissuhtest tegutseda iseseisvate vastutavate töötajatena, volitatud töötajatena või alamtöötajatena ning töötlevad isikuandmeid vastavalt oma tingimustele ja kohaldatavatele õigusaktidele.

4.3. EIS:

- pakub tehnilist liidestust ja vahendab andmevahetust;
- ei määra kolmandate teenusepakkujate poolt läbiviidava isikuandmete töötlemise eesmärgi ega põhivahendeid ulatuses, milles vastavad teenusepakkujad tegutsevad iseseisvate vastutavate töötajatena.

4.4. Klient annab käesolevaga EISile üldise volituse kasutada teenuse osutamiseks vajalikke kolmandaid teenusepakkujaid ja alamtöötlejaid.

4.5. EIS tagab, et teenuse osutamisel kasutatavad kolmandad teenusepakkujad järgivad kohaldatavaid andmekaitsealaseid õigusakte ning rakendavad isikuandmete kaitseks asjakohaseid tehnilisi ja korralduslikke turvameetmeid.

4.6. EISil on õigus kolmandaid teenusepakkujaid, volitatud töötlejaid lisada, asendada või muuta vastavalt teenuse tehnilistele, turvalisuse või ärilistele vajadustele.

4.7. Teave teenuse osutamisel kasutatavate oluliste kolmandate teenusepakkujate kohta on avaldatud kasutajakeskkonnas.

4.8. Kui kolmas teenusepakkuja asub väljaspool Euroopa Majanduspiirkonda või toimub isikuandmete edastamine väljapoole Euroopa Majanduspiirkonda, tagab EIS, et andmete edastamine toimub kooskõlas kohaldatavate andmekaitsealaste õigusaktidega, sealhulgas vajadusel Euroopa Komisjoni standardsete lepingutingimuste või muu asjakohase õigusliku mehhanismi alusel.

4.9. EIS vastutab isikuandmete edastamise õiguspärasuse eest oma teenuse raames.

4.10. EIS ei vastuta kolmandate teenusepakkujate otsuste, autentimistulemuste, biomeetriliste hinnangute, teenuse katkestuste, otsustusloogikate ega nende poolt läbiviidava isikuandmete töötlemise õiguspärasuse eest ulatuses, milles selline töötlemine toimub väljaspool EISi platvormi või väljaspool EISi kontrolli all olevaid süsteeme.

## 5. Andmeedastus

5.1. Teenuse osutamisel võib toimuda isikuandmete edastamine väljapoole Euroopa Majanduspiirkonda, kui see on vajalik teenuse tehniliseks toimimiseks, turvalisuse tagamiseks, autentimis- või isikutuvastusteenuse osutamiseks või teenusega seotud tugiteenuste kasutamiseks.

5.2. EIS tagab, et isikuandmete edastamine väljapoole Euroopa Majanduspiirkonda toimub kooskõlas kohaldatavate andmekaitsealaste õigusaktidega ning üksnes juhul, kui:

- Euroopa Komisjon on vastava riigi kohta teinud piisava kaitsetaseme otsuse;
- kasutatakse Euroopa Komisjoni kinnitatud standardseid lepingutingimusi (*Standard Contractual Clauses*);
- või kasutatakse muud kohaldatavate õigusaktidega lubatud andmeedastusmehhanismi.

5.3. EIS rakendab mõistlikke tehnilisi ja korralduslikke meetmeid, et tagada isikuandmete kaitse ka piiriülese edastamise korral.

5.4. Klient nõustub, et teenuse osutamisel kasutatavad kolmandad teenusepakkujad või alamtöötlejad võivad töödelda isikuandmeid väljaspool Euroopa Majanduspiirkonda käesolevas punktis sätestatud tingimustel.

## 6. Isikuandmete töötlemine koostöös Kliendiga

6.1. EIS ja Klient võivad autentimis- või isikutuvastustoimingu tehnilise läbiviimise käigus tegutseda piiratud ulatuses kaasvastutavate töötlejatena üksnes määral, mis on vältimatult vajalik kasutaja autentimis- või isikutuvastustoimingu tehniliseks

läbiviimiseks. Pärast autentimis- või isikutuvastustulemuse edastamist Kliendile tegutseb Klient iseseisva vastutava töötlejana.

## 6.2. Vastutuse jaotus:

- EIS vastutab:
  - teenuse tehnilise toimimise ja turvalisuse eest enda platvormil;
  - autentimise ja tuvastamise protsessi eest;
  - andmete töötlemise eest oma platvormil;
  - EIS töötleb kliendi kasutaja isikuandmeid ulatuses, mis on vajalik kliendi poolt kasutatava autentimis- või isikutuvastusmeetodi toimimiseks ja teenuse osutamiseks.
- Klient vastutab:
  - isikuandmete töötlemise eest oma süsteemides ja e-teenustes;
  - kasutaja selge ja arusaadava teavitamise eest enne eeID teenusesse suunamist, sealhulgas kuhu kasutaja suunatakse ja mis eesmärgil tema isikuandmeid töödeldakse;
  - selle eest, et kasutajale esitatakse piisav ja arusaadav teave isikuandmete töötlemise kohta kliendi e-teenuses;
  - andmesubjekti õiguste tagamise eest oma e-teenuse raames.

6.3. Kasutaja võib oma õiguste teostamiseks pöörduda nii EISi kui ka Kliendi poole.

6.4 EIS ei määra Kliendi e-teenuses läbiviidava isikuandmete töötlemise eesmärke, õiguslikku alust, säilitamistähtaegu ega muid põhilisi töötlemisvahendeid. Klient otsustab iseseisvalt, millal, millisel õiguslikul alusel ja millise funktsionaalsuse raames eeID teenust kasutatakse.

6.5 Kui Klient kasutab videotuvastuse, biomeetrilise võrdluse või muu kõrgendatud privaatsusriskiga isikutuvastuse funktsionaalsust sisaldavat teenust (nt Veriff teenuseid), vastutab Klient selle eest, et:

- andmesubjektile esitatakse enne teenuse kasutamist selge ja arusaadav teave biomeetriliste, näokujutise või muude isikutuvastamiseks kasutatavate andmete töötlemise kohta;
- isikuandmete töötlemiseks esineb kohane õiguslik alus vastavalt kohaldatavatele õigusaktidele;

6.6 Klient vastutab hinnangu andmise eest, kas eeID teenuse või selle kaudu kasutatavate autentimis- või isikutuvastusteenuste kasutamine kliendi e-teenuses nõuab andmekaitsealase mõjuhinnangu (DPIA) läbiviimist IKÜM artikli 35 tähenduses. Kui andmekaitsealase mõjuhinnangu läbiviimine on nõutav, vastutab Klient selle koostamise eest. EIS teeb Kliendiga mõistlikus ulatuses koostööd ja annab vajadusel teenuse tehnilise toimimise kohta vajalikku teavet.

## 7. Poolte rollid isikuandmete töötlemisel

7.1. Pooled mõistavad ja nõustuvad, et nende rollid isikuandmete töötlemisel võivad erineda sõltuvalt konkreetsest töötlemistoimingust ja kasutatavast teenusest.

7.2. EIS tegutseb iseseisva vastutava töötlejana:

- eeID platvormi ja kasutajakeskkonna opereerimisel;
- teenuse tehnilise toimimise, turvalisuse ja logimise tagamisel;
- EISi süsteemides töödeldavate isikuandmete töötlemisel;
- teenuse kasutamise statistika, turvalisuse ja väärkasutuse ennetamise, uurimise ja lahendamise eesmärkidel läbiviidava töötlemise osas.

7.3. Klient tegutseb iseseisva vastutava töötlejana:

- oma e-teenuse, infosüsteemi või kliendirakenduse toimimise raames;
- kasutajatele teenuse osutamisel;
- kasutajate isikuandmete töötlemisel kliendi süsteemides;
- kliendi määratud eesmärkidel läbiviidava andmetöötluse osas.

7.4. Pooled võivad autentimis- või isikutuvastustoimingu tehnilise läbiviimise käigus tegutseda piiratud ulatuses kaasvastutavate töötlejatena IKÜM artikli 26 tähenduses üksnes ulatuses, mis on vajalik:

- kasutaja autentimis- või isikutuvastuspäringu vahendamiseks;
- autentimis- või isikutuvastustulemuse edastamiseks;
- teenuse turvalisuse ja töökindluse tagamiseks.

7.5. Kui teenuse osutamisel kasutatakse kolmanda osapoole isikutuvastusteenust või videotuvastuse lahendust (näiteks Veriff teenuseid), võib vastav teenusepakkuja tegutseda iseseisva vastutava töötlejana või volitatud töötlejana vastavalt tema teenuse tingimustele ja konkreetsele töötlemissuhtele.

7.6. EIS ei määra Kliendi e-teenuses läbiviidava isikuandmete töötlemise eesmärke, õiguslikke aluseid ega säilitamistähtaegu ning ei vastuta Kliendi iseseisva andmetöötluse eest väljaspool EISi platvormi.

7.7 Pooled teavitavad üksteist põhjendamatu viivitusega isikuandmete rikkumisest või turvaintsidendist, mis võib mõjutada teise Poole töödeldavaid isikuandmeid või teenuse turvalisust.

## 8. Turvalogi

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

8.1.1. teenuse väärkasutamise, sh identiteedivarguste ja nende katsete, samuti küberrünnakute avastamiseks ja uurimiseks;

8.1.2. tehniliste tõrgete avastamiseks ja kõrvaldamiseks. Tehniline tõrge võib olla nii riist- kui ka tarkvara viga, võrguühenduse viga jms;

8.1.3. teenustega liidestatud e-teenuste omanike s.t asutuste poolt raporteeritud tehniliste probleemide põhjuste väljaselgitamiseks;

8.1.4. kasutajate pöördumiste (teated võimalike turvaprobleemide või tehniliste rikete kohta) menetlemiseks.

8.2. Logile juurdepääs on rangelt vajaduspõhine. Ligi pääsevad ainult teenuse käitamise otseselt seotud süsteemi- ja teenusehaldurid, vajadusel ka turvaintsidentide uurimisega tegelevad ametiisikud.

8.3. Autentimisi soovitame logida ka kliendirakenduse poolel. See on vajalik nii tehniliste tõrgete kui ka teenuse väärkasutuse tuvastamisel ja uurimisel.

## 9. Andmete säilitamine ja turvalisus

9.1. Isikuandmeid säilitatakse ainult nii kaua, kui see on vajalik:

- teenuse osutamiseks;
- turvalisuse tagamiseks;
- seadusest tulenevate kohustuste täitmiseks.

9.2 Varundusprotsess käivitatakse vähemalt korra ööpäeva jooksul. Kõikide teenuse komponentide andmete (konfiguratsioon, andmebaas, logid) tagavarakoopiaid säilitatakse sama põhimõtte alusel – 7 päeva / 4 nädalat / 12 kuud. Taastada on võimalik jooksva nädala päevade, jooksva kuu nädala lõpu või viimase 12 kuu lõpu seisuga salvestatud andmed.

9.3. EISI teenuses loodud kasutajakonto kehtivus on seotud kasutaja viimase autentimise ajaga. Kasutajakonto loetakse mitteaktiivseks, kui kasutaja ei ole teenust kasutanud viie (5) aasta jooksul alates viimasest edukast autentimisest. Mitteaktiivse kasutajakonto andmeid säilitatakse ja varundatakse vastavalt varundusprotsessile.

9.4. Andmete kaitsmiseks kasutatakse:

- krüpteeritud andmesidekanaleid;
- juurdepääsupiiranguid;
- logimist ja seiret.

9.5. Ligipääs andmetele on ainult volitatud isikutel.

## 10. Andmesubjekti õiguste teostamine

10.1. Pooled tagavad andmesubjekti õiguste teostamise kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2016/679 (IKÜM) ning kohaldatavate õigusaktidega oma vastutusalas ja oma süsteemides töödeldavate isikuandmete osas.

10.2. Kumbki Pool vastutab iseseisvalt:

- tema süsteemides ja teenustes töödeldavate isikuandmete õigsuse, töötlemise õiguspärasuse ja turvalisuse eest;
- andmesubjekti taotluste menetlemise eest ulatuses, milles taotlus puudutab tema hallatavaid süsteeme, teenuseid või andmeid;
- IKÜMist tulenevate kohustuste täitmise eest oma vastutusalas.

10.3. Kui Pool saab andmesubjektilt taotluse, kaebuse või muu pöördumise, mis puudutab täielikult või osaliselt teise Poole poolt töödeldavaid isikuandmeid või teise

Poole vastutusala, edastab Pool vastava pöördumise teisele Poolele põhjendamatu viivitusega, kuid võimalusel hiljemalt viie (5) tööpäeva jooksul.

10.4. Pooled teevad mõistlikku koostööd andmesubjekti õiguste teostamise võimaldamiseks, sealhulgas:

- vahetavad vajalikku teavet;
- annavad üksteisele mõistlikus ulatuses abi;
- kooskõlastavad vajadusel vastuseid andmesubjektidele või järelevalveasutustele.

10.5. EIS vastutab üksnes EISi platvormil ja süsteemides töödeldavate isikuandmete eest ning ei vastuta Kliendi e-teenustes, infosüsteemides ega muudes kliendi hallatavates keskkondades toimuvate töötlemistoimingute eest.

10.6. EISil puudub õigus ning tehniline võimalus kustutada, parandada või piirata Kliendi süsteemides või e-teenustes töödeldavaid isikuandmeid.

10.7. Klient vastutab selle eest, et andmesubjektidele oleks enne eeID teenuse kasutamist esitatud nõuetekohane teave isikuandmete töötlemise kohta Kliendi e-teenuses, sealhulgas teave:

- isikuandmete töötlemise eesmärkide kohta;
- kasutatavate autentimis- või isikutuvastusmeetodite kohta;
- võimalikust andmete edastamisest kolmandatele teenusepakkujatele;
- andmesubjekti õiguste teostamise võimalustest.

10.8. Käesolevad andmekaitsetingimused ei piira andmesubjekti õigust pöörduda oma õiguste teostamiseks otse kummagi Poole poole ega esitada kaebust pädevale järelevalveasutusele.

## **11. Turvalogide väljastamine**

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