Uuringu andmekaitsealane mõjuhinnang

Käesolev andmekaitsealane mõjuhinnang on tehtud põhjusel, et Euroopa isikuandmete kaitse üldmääruse (2016/679, edaspidi GDPR) artikkel 35 lõiked 1 ja 3 nõuab enne ulatuslikku eriliiki isikuandmete (terviseandmeid) töötlemist kavandatavate isikuandmete töötlemise toimingute mõju hindamist isikuandmete kaitsele.

# Kokkuvõte andmekaitsealase mõjuhinnangu tulemustest

Käesolev andmekaitsealane mõjuhinnang on läbi viidud uurimisprojekti „**Epilepsia epidemioloogia Eestis ja masinõppe kasutamise võimalused epilepsia epidemioloogilistes uuringutes**“ kohta. Uurimisprojekt hõlmab riiklikest andmekogudest pärit terviseandmete töötlemist teaduslikuks kasutuseks.

Andmekaitsealane mõjuhinnang on läbi viidud ajavahemikus 20.08.2024 – 02.10.2024 ning kehtib kuni uurimisprojektis kasutatud andmete hävitamiseni. Juhul, kui muutuvad mõjuhinnangu aluseks olnud asjaolud, siis mõjuhinnangut täiendatakse vastavalt.

Kokkuvõttes leiavad mõjuhinnangu koostajad, et uurimisprojektis on kasutusel tõhusad riskimaandamise mehhanismid ja rakendatud meetmete tulemusena ei teki andmesubjekti õigustele suurt ohtu isikuandmete kaitse üldmääruse (2016/679/EU) artikkel 35 lõike 1 tähenduses.

Mõjuhinnang on kooskõlastatud Tartu Ülikooli andmekaitse peaspetsialistiga.

# Sissejuhatus

Tartu Ülikool (TÜ) on avalik-õiguslik ning vanim ja suurim Eesti ülikool. Tartu Ülikooli üheks peamiseks eesmärgiks on edendada teadust, kuid spetsiifilisemalt ka edendada Eestit ja tema rahvast uurivaid teadusi ning eestikeelset haridust.

Tartu Ülikooli neljast valdkonnast on konkreetselt meditsiinile keskendunud meditsiiniteaduste valdkond. Samas on tervisevaldkond muutumas järjest interdistsiplinaarsemaks ning meditsiiniga on tihedalt seotud ka loodusteaduste valdkond ja arvutiteaduse instituut arendab terviseandmetel rakendamiseks andmeteaduse meetodeid, s.h masinõpet.

Käesolevas mõjuhinnang käsitleb andmete töötlemist **„Epilepsia epidemioloogia Eestis ja masinõppe kasutamise võimalused epilepsia epidemioloogilistes uuringutes“** uuringu raames, mis on kooskõlas WHO IGAP tegevuskavaga (sektoritevaheline globaalne tegevuskava epilepsia ja teiste neuroloogiliste haiguste osas 2022-2031; Intersectoral lobaal action plan on epilepsy and other neurological disorders https://www.who.int/publications/i/item/9789240076624), mida on allkirjastanud ka Eesti ja mille edukaks elluviimiseks on vaja omada kaasaegseid andmeid epilepsia epidemioloogia, diagnostika ja ravipraktika kohta Eesti riigis. Täiskasvanute epilepsia epidemioloogiat Eestis uuris viimati dr. Andre Õun rohkem kui veerand sajandit tagasi (1994-1997). Selle pika aja jooksul on toimunud suured arengud nii epilepsia, kui üleüldiselt neuroloogiliste haiguste käsitluse praktikas.

Antud uuringu põhieesmärgiks on välja selgitada kaasaegsed aktiivse epilepsia haigestumus- ja levimusnäitajad Tartu täiskasvanutel ning võrrelda saadud andmeid 27 aastat tagasi dr. Andre Õuna poolt tehtud epidemioloogilise uuringu tulemustega.

Haigestumusuuringu kriteeriumid: Tartu Linna elanikud, kellel esines perioodil 1. jaanuar 2021- 31. detsember 2023 indeks-epileptiline hoog ja kes olid selle hoo ajaks ≥20 aastat vanad.

Levimusuuringu kriteeriumid: Tartu linna elanikud, kes olid levimuskuupäevaks (1. jaanuar 2024) ≥20 aastat vanad ja kellel oli enne levimuspäeva olnud epilepsia diagnoos ja vähemalt 1 epileptiline hoog eelneva viie aasta jooksul või nad regulaarselt tarvitasid epilepsiaravimeid.

Lisaks on eesmärk välja töötada masinõppel põhinevaid algoritme, et tuvastada tekst-andmete massiivist korduvate epilepsia epidemioloogiliste uuringute läbiviimiseks vajalikku informatsiooni ja hinnata haigestumus- ja levimusnäitajaid kogu Eesti täiskasvanud rahvastikus samal perioodil.

## Mõjuhinnangu läbiviimisest

### Läbiviimise aeg

Käesolev andmekaitsealane mõjuhinnang on läbi viidud ajavahemikul 20.08.2024 – 02.10.2024.

### Mõjuhinnangu ulatus

Käesolev andmekaitsealane mõjuhinnang on koostatud uuringus „**Epilepsia epidemioloogia Eestis ja masinõppe kasutamise võimalused epilepsia epidemioloogilistes uuringutes**“ kasutatavate andmete elutsükli kohta Tartu Ülikoolis.

### Metoodika

Käesoleva andmekaitsealase mõjuhinnangu loomisel on kasutatud riskide identifitseerimisel ja hindamisel põhinevat metoodikat. Mõjude hindamisel võetakse arvesse kirjeldatud andmetöötlemise iseloomu, ulatust ja konteksti. Riskid on leitud ja kirjeldatud andmetöötluse ohustsenaariumite hindamisest lähtuvalt. Riskide hindamisel on hinnatud skaalal (0-väga madal; 4-väga kõrge) kahte tegurit:

* riski realiseerumise tõenäosus;
* riski realiseerumise mõju.

Üldine riski tase leitakse kahe skaala ristumispunktis vastavalt alltoodud joonisele ja tabelile. Näiteks kui tõenäosus on 3 ja mõju 2, siis riski tase on 5 ehk keskmine.

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| Riski tase | |
| Tulemus | Kirjeldus |
| 6-8 | Kõrge |
| 3-5 | Keskmine |
| 0-2 | Madal |

# Projektipõhise infosüsteemi kirjeldus

Uuringu andmestikku hoitakse ja kõik teisendused/analüüsid teostatakse Tartu Ülikooli teadusarvutuste keskuse poolt pakutavas sensitiivsete andmete privaatses uurimiskeskkonnas (SAPU). Projekti käigus kasutatakse eraldiseisvat SAPU keskkonda, mis ei ole seotud teiste SAPU keskkondadega. Detailne info Tartu Ülikooli teadusarvutuste keskuse kohta on leitav aadressil <https://hpc.ut.ee> ja lisainfo sensitiivsete andmete privaatse uurimiskeskkonna (SAPU) koht on leitav aadressil <https://docs.hpc.ut.ee/public/services/SAPU/> (inglise keeles).

## Kasutajate haldus

Projekti käigus kasutatavasse SAPU keskkonda (andmepuur) luuakse spetsiaalsed ja eraldiseisvad kasutajakontod ainult projektijuhi taotlusel ja heakskiidul vastavalt vajadusele (nt Uurimisgruppi lisandub uusi uurijaid). SAPU keskkond on selleks volitatud isikutele kättesaadav ainult aktiivse analüüsi faasis ning muul ajal on keskkond välja lülitatud ning sinna ei ole võimalik siseneda ka kasutajakonto olemasolu korral. Kolmandatel isikutel (kaasa arvatud Tartu Ülikooli teistel töötajatel) puudub juurdepääs kasutatavasse SAPU keskkonda.

SAPU keskkonnas eristatakse nelja erinevat kasutajarolli:

* *Cloud operator* (administraatori õigused) - SAPU tehniline administraator, seda rolli täidab TÜ teadusarvutuste keskus - hoolitseb turvalisuse, monitoorimise ülesannete eest, vastutab, et server töötab.
* *Data owner* (otsene ligipääs masinale ja monitoorimisele) - toovad andmed SAPU masinasse sisse ning peavad heaks kiitma kõik andmete välja liigutamised SAPU masinast.
* *Data custodian* (otsene ligipääs masinale ja monitoorimisele) - andmeomaniku tehniline esindaja - tegeleb peaasjalikult tehniliste küsimustega ja vajadusel aitab pilve operaatorit.
* *Data analyst* (ligipääs üksnes läbi virtuaalse töölaua) - analüütik, töötleb andmeid.

## Teadaolevad turvameetmed

* Andmete edastus andmeandjate poolt toimub krüpteeritult läbi turvalise SFTP serveri, mis on üles seatud Tartu Ülikooli teadusarvutuste keskuse poolt või kasutades andmeallikate tavapäraseid andmete väljastamise viise vastavalt nende sisemistele protseduurireeglitele (enamasti konkreetsele juhtivuurijale parooliga ligipääsetav kataloog andmeallika serveris, andmefail on krüpteeritud).
* Analüüsiks kasutatakse Tartu Ülikooli teadusarvutuste keskuse poolt pakutavat sensitiivsete andmete privaatset uurimiskeskkonda (SAPU), millele on piiratud ligipääs vaid eetikaloal loetletud uurijatele.
* Kasutusel on füüsilise ja infotehnoloogilised turvameetmed, mida on täpsemalt kirjeldatud mõjuhinnangu lõpus.

## Süsteemi kasutusotstarve

Sensitiivsete andmete privaatne uurimiskeskkond (SAPU) on Tartu Ülikooli teadusarvutuste keskuse poolt spetsiaalselt loodud ja pakutav andmetöötluskeskkond, kus analüütikud saavad töötada tundlike andmete kallal, vähendades võimalikku andmete volitamata kopeerimist, ülekandmist või masinatest välja võtmist, pakkudes kõrgemat turvaklassi kui tavaline suure jõudlusega arvutusklaster.

## SAPU kõrgetasemeline arhitektuur

A diagram of a computer network

Description automatically generated

### SAPU andmevärav

Kuna analüütikud vajavad võimalust SAPU masinasse viia andmeid, skripte ja muud teavet ning samuti on vajalik SAPU masinast andmeid välja viia, siis on kasutusele võetud S3 Object Storage põhised eeskirjad, mis on kujutatud järgmisel joonisel:

A diagram of a computer

Description automatically generated with medium confidence

### Graafiline kasutajaliides

RDP või masina avalikustamine internetis kätkeb endas mitmeid infoturbe riske ja nende maandamiseks on kasutusele võetud puhverserver. Kasutatakse avatud lähtekoodiga tehnoloogiat Apache Guacamole.

A diagram of a network

Description automatically generated

### Autentimine ja autoriseerimine

SAPU’l on eraldiseisev LDAP server, millega luuakse ühendus identiteedi ja juurdepääsu haldamiseks.

A diagram of a network

Description automatically generated

## Andmestiku elutsükkel

Andmestiku elutsükkel on järgmine:

1. Andmeandjad edastavad oma infosüsteemidest vajalikud andmed Tartu Ülikooli uurijale.
2. Uurimisgrupi uurija tõstab andmed SAPU-sse.
3. Uurimisgrupi liikmed töötlevad SAPU-s olevaid andmeid uurimisprojekti tarbeks.
4. Vajadusel toimub tulemuste väljastamine SAPU-st.
5. Uuringu lõppedes SAPU koos andmetega kustutatakse. Kustutatakse ka kõik SAPU ja andmete varukoopiad.

# Isikuandmete töötlemise toimingud

## Isikuandmete kogumine

Käesolevas uuringus uusi isikuandmeid ei koguta ja andmesubjektidega ühendust ei võeta. Kasutatakse juba olemasolevaid terviseandmeid teadusuuringute läbiviimise eesmärgil. Vastavalt isikuandmete kaitse seadusele § 6 lg 1 võib teadusuuringu vajaduseks isikuandmeid töödelda andmesubjekti nõusolekuta, kui need on pseudonüümitud. Andmed pseudonüümitakse käesolevas uuringus enne Uurimisgrupini jõudmist andmeallikate poolt.

Vaatamata sellele, et andmed on pseudonüümitud ega sisalda isiku otsest tuvastamist võimaldavaid tunnuseid, käsitletakse uuringu andmeid järgmistes peatükkides tulenevalt nende tundlikust iseloomust ning üldmäärusest sätestatust kui isikuandmeid.

## Isikuandmete pseudonüümimine ja edastamine

### Valimi moodustamine ja pseudonüümide moodustamine

Valim moodustatakse Tervisekassa andmete põhjal. Andmesubjektideks on kõik Eesti elanikud kes:

* on sündinud enne 01.01.2004; ja
* olid 01.01.2024 seisuga elus või surid vahemikus 01.01.2021-31.12.2023; ja
* kehtib vähemalt üks järgmistest tingimustest:
  + on retseptikeskuse andmeil ostnud kasvõi ühe korra elus ravimeid diagnoosiga „epilepsia“ (G40-G41 koos alamkoodidega); või
  + on raviarvetel diagnoositud kas põhi- või kaasuva haigusena epilepsia (G40-G41), teadvusekaotus (R55), vapluskrambid (R56), karotiidsiinussünkoop (G90), kramp ja spasm (R25.2) või kuumasünkoop (süvaminestus) (T67.1). Nimetatud diagnoosid võivad olla antud ka alamkoodidena.

### Pseudonüümide moodustamine ja andmeallikatega jagamine

Tervisekassa koostab valimisse kuuluvatele isikutele tagasipööramatu juhusliku unikaalse pseudonüümi. Tervisekassa loob valimisse kuuluvate isikute isikukood-pseudonüüm vastavustabeli ja krüpteerib selle TEHIK ja Rahvastikuregistri nimele (uurijad valimisse kuuluvate isikute isikukoode ega muid otseseid isiku tuvastamist võimaldavaid andmeid ei saa). Tervisekassa ja TEHIK säilitavad vastavustabeli 10 aastaks (kuni 31.12.2034), et tulevikus oleks vastavate uuringute raames (koos vastavate eetikakomiteede lubadega) selle alusel võimalik hinnata Tartu epilepsiaga haigete suremust. Rahvastikuregister kustutab vastavustabeli pärast uurijatele andmete väljastamist.

### Andmete töötlus enne Uurimisgrupile väljastamist

Andmeallikad väljastavad üksnes valimisse kuuluvate isikute pseudonüümitud andmed.

Nende isikute kohta väljastatakse uurimisgrupile andmed järgmistest andmekogudest:

Tervisekassast:

1. valimisse kuuluvate isikute tabeli, milles on isikute kohta järgmised andmed: pseudonüüm, sugu, sünniaasta ja sünnikuu, surma kuupäev (kui surnud), kas elukoht Tartus (jah/ei).
2. valimisse kuuluvate isikute kõik nende 01.01.2019-31.12.2023 väljakirjutatud ja väljaostetud digiretseptid, mille diagnoos on G40-G41 (koos alamdiagnoosi koodidega):
   1. Patsiendi pseudonüüm
   2. Retsepti koostamise aeg
   3. Diagnoosi kood ja nimetus
   4. Välja kirjutatud ravimi toimeaine (toimeaine 1, toimeaine 2, toimeaine 3) nimetus
   5. Realiseeritud toimeaine (toimeaine 1, toimeaine 2, toimeaine 3) nimetus
   6. Välja kirjutatud ravimi ravimvormi kood ja seletus
   7. Realiseeritud ravimi ravimvormi kood ja seletus
   8. Toimeainete 1, 2, 3 sisaldus ja ühik (nt 0,4 mg 1ml)
   9. Realiseeritud toimeainete 1, 2, 3 sisaldus ja ühik (nt 0,4 mg 1ml)
   10. Välja kirjutatud ravimi ATC kood
   11. Realiseeritud ravimi ATC kood
   12. Välja kirjutatud ravimi koguhulk (ühikute kogus ühes pakendis ja ühe ühiku suurus pakendis)
   13. Realiseeritud ravimi koguhulk (ühikute kogus ühes pakendis ja ühe ühiku suurus pakendis)
   14. Välja kirjutatud ravimpreparaatide arv (pakendite arv)
   15. Realiseeritud ravimpreparaatide arv (pakendite arv)
   16. Annustamine (ravikuuri tüüp, ravikuuri pikkus päevades, tükkide arv, tükkide ühik, kordade arv ja kordade ühik, annustamisskeemi perioodi pikkus).
   17. Retsepti staatuse kood ja nimetus
   18. Annulleerimise põhjus (kood ja seletus)
   19. Väljastaja info (müümise aeg, apteegi kood)
   20. Ravimi välja ostmise kuupäev

Tervise infosüsteemist:

1. valimisse kuuluvate isikute kõik med. dokumendid mille diagnooside hulgas on G40-G41 (koos alamdiagnoosi koodidega) või R55-R56 (koos alamdiagnoosi koodidega), karotiidsiinussünkoop G90 koos alamdiagnoosi koodidega, kramp ja spasm R25.2 või kuumasünkoop (süvaminestus) T67.1. Nendest dokumentidest on eemaldatud isikuandmete plokk, kuid on aru saada, millise pseudonüümiga milline dokument on seotud. Alates eelmise kümnendi algusest on kogu meditsiiniline dokumentatsioon Eestis registreeritud digitaalsel kujul, seega TEHIKult saadud digitaalsetes dokumentides peab olema kajastatud info parimal võimalikul kujul uuritavate epilepsia diagnoosist, kulust, etioloogiast, ravist.

Rahvastikuregister:

1. valimisse kuuluvate isikute kohta nende elukoha info: pseudonüüm, kuupäev, kas elukoht Tartus (jah/ei). Kõigi isikute kohta on siin vähemalt üks rida kuupäevaga 01.01.2021, aga kui elukoht on enne 2024. a muutunud, siis nende kohta on mitu rida.

### Andmete üleandmine Uurimisgrupile

Andmete edastus toimub krüpteeritult läbi turvalise SFTP serveri, mis on üles seatud Tartu Ülikooli teadusarvutuste keskuse poolt või kasutades andmeandjate tavapäraseid andmete väljastamise viise vastavalt nende sisemistele protseduurireeglitele (enamasti konkreetsele juhtivuurijale parooliga ligipääsetav kataloog andmeallika serveris koos krüpteeritud andmefailiga).

### Andmete uuendamine

Andmestiku andmeid ei uuendata.

## Andmete säilitamine

Kõik andmeid säilitatakse Tartu Ülikooli teadusarvutuste keskuses vastavas projekti põhises privaatses SAPU privaatserveris, millele on juurdepääs vaid eetikaloal mainitud isikutel. Vajadusel säilitatakse andmed krüpteeritud kujul.

Andmeallikatelt saadud algandmed paigaldatakse SAPU-s spetsiaalselt kirjutuskaitstud kausta, et vältida andmete juhuslikku hävimist või kahjustumist. Kuigi uuringumeeskonnale ei väljastata patsientide isikuandmeid (andmed on pseudonüümitud), võib dokumentide vabateksti osades isikuandmeid siiski sisalduda. Seetõttu kasutatakse andmetel esimese tegevusena TÜ poolt arendatud anonüümimisrakendust, mis tuvastab ja asendab algandmete vabatekstilistest dokumendiosadest isikunimed, aadressid, telefoninumbrid, isikukoodid, kui neid seal peaks leiduma. Edasine töötlus käib ainult nende andmete pealt ning algselt saadud algandmetele pääsevad ligi üksnes juhtivuurijad ja *data custodian* rollis (vt allpool) olev kasutaja, et anonümiseerimisrakendust vajadusel uuesti kasutada.

SAPU-st tehakse regulaarselt krüpteeritud varukoopiaid Tartu Ülikooli teadusarvutuste keskuse lindirobotile, mis asub füüsiliselt teises asukohas (andmekeskuses).

### Säilitamise tähtajad

Andmeid säilitatakse kuni projekti eesmärkide täitmiseni, kuid maksimaalselt kuni uuringuprojekti lõpuni: 31.12.2034.

Kui uuringu käigus tekib põhjendatud vajadus andmeid säilitada kauem, esitatakse enne uuringu lõppu eetikakomiteele vastavasisuline taotlus.

### Hoiustamisel kasutatavad turvameetmed

Tartu Ülikooli teadusarvutuste keskus järgib infrastruktuuri haldamisel ISKE M taseme nõudeid. Andmeid ja vaheandmeid hävitatakse vajadusel vastavalt ISKE H turbeastmega andmete hävitamise nõuetele. Tartu Ülikooli teadusarvutuste keskus käsitleb kõiki teenuse pakkumise käigus teatavaks saavaid/käsitletavaid andmeid konfidentsiaalsetena.

Seoses 2022. aasta lõpus kehtima hakanud „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ määruse ja „Eesti infoturbestandard“ määrusega on Tartu Ülikool ja ka Tartu Ülikooli teadusarvutuste keskus kohustatud järgima Eesti Infoturbestandardit ning regulaarselt läbi viima Eesti infoturbestandardi järgimise auditeid. Tartu Ülikool peab esimese auditi läbima vähemalt 3 aasta jooksul (ehk enne 2025. a lõppu) ning käesoleval hetkel selle nimel ka tegutsetakse.

### Kuidas välditakse andmete juhuslikku hävimist või kahjustumist?

* Andmetest tehakse regulaarseid krüpteeritud varukoopiaid.
* Regulaarselt teostatakse serverite turvatestimist, uuendamist ja monitoorimist.
* Serverid on varustatud katkematu toiteallikaga (UPS).
* Kasutusel on füüsilised ja organisatoorsed turvameetmed, mis takistavad selleks volitamata isikute füüsilist juurdepääsu serveritele.
* Kasutajal puudub SAPU keskkonnast juurdepääs internetile.
* Kasutajal puudub SAPU keskkonnas õigus installeerida programme.
* SAPU keskkonda saavad siseneda ainult selleks vastavaid õigusi omavad kasutajad.
* Kasutajaid juhendatakse ja koolitatakse SAPU keskkonna kasutamise osas.

### Logid, turvakoopiad

Andmete töötlus toimub SAPU keskkonnas, mis rangelt piirab kasutajate võimalust andmeid serverist välja kopeerida ning võimaldab vastutavatel uurijatel jälgida kõikide kasutajate tegevusi. Logitakse kõik kasutaja tegevused SAPU keskkonnas ning lisaks salvestatakse jooksvalt ka kasutaja ekraanipilti (video). Kasutajad on logidest ja ekraanipildi salvestamisest teadlikud ning see toimib ka heidutava meetmena.

Andmetest tehakse üks kord nädalas regulaarseid varukoopiad vastavalt Tartu Ülikooli teadusarvutuste keskuse varundamise korrale. Varundamine toimub Tartu Ülikooli teadusarvutuste keskuse lindirobotile, mis asub füüsiliselt teises asukohas (andmekeskuses). Varukoopiad on spetsiaalselt krüpteeritud, alles hoitakse viimast kolme varukoopiat. Varukoopiate tegemisel kasutatakse inkrementaalset varukoopiat ja on tagatud, et eelnevaid varukoopiaid ei ole võimalik muuta.

### Arhiveerimine

Projekti raames toimub andmete varundamine, kuid ei toimu andmete arhiveerimist.

## Andmete kasutamine

Andmeid kasutatakse üksnes Uurimisgrupi poolt ainult SAPU serveris ja üksnes käesolevas mõjuhinnangus kirjeldatud uuringu läbiviimiseks.

### Uurimisgrupp

Uurimisgrupi koosseis on käesoleva mõjuhinnangu koostamise hetkel järgmine:

|  |  |  |
| --- | --- | --- |
| Nimi | Roll projektis | Roll SAPU serveris |
| Aleksei Rakitin | Juhtivuurija, teadur | Data owner |
| Raivo Kolde | Juhtivuurija, kaasprofessor | Data owner |
| Sulev Reisberg | Juhtivuurija, teadur | Data custodian |
| Sven Laur | Juhtivuurija, kaasprofessor | Data analyst |
| Hendrik Šuvalov | Uurija, nooremteadur | Data analyst |
| Marek Oja | Uurija, teadur | Data custodian |
| Sulev Haldre | Juhtivuurija, kaasprofessor | Data analyst |
| Sander Kütisaar (TÜ teadusarvutuskeskus) | SAPU pilve operaator, tagab SAPU serveri töö, kuid ei kasuta andmeid, ei tohi neid vaadata, avada jne. | Cloud peraator |

Uurimisgrupi koosseis ja rollid võivad projekti käigus juhtivuurijate heakskiidul kindla protsessi alusel täieneda. Isikkoosseisu muutmiseks esitatakse eetikakomiteele vastavasisuline jätkutaotlus.

Andmete väljastamine SAPU serverist saab toimuda üksnes *“data owner”* rollis uurija heakskiidul ja see juhtub üldjuhul uurimistulemuste avaldamisel nt teaduspublikatsioonis. Väljastuse heakskiitmisel kontrollib uurija, et väljastatavad andmed on kooskõlas uuringu taotluses kirjeldatud eesmärkide ja sisuga. Uurimisgrupp avaldab üksnes statistilisi tulemusi, kus on tagatud k >= 5 anonüümsus. Uurimisgrupp ei avalda ega jaga ühegi koostööpartneritega üksikpatsientide andmeid ega pseudonüüme. Kõikide avaldatavate andmestike kohta annab oma heakskiidu vastutav uurija.

Uuringute tulemused publitseeritakse nii Eesti kui rahvusvahelistes teadusajakirjades (eelistatult vabalt kättesaadavate artiklitena), konverentsidel ja ettekannetel, üliõpilaste lõputöödes. Erakapitalil põhinevate uuringute puhul otsustab avaldamise uuringu rahastaja.

## Andmete kustutamine

Andmed kustutatakse projekti lõpus (31.12.2034) koos SAPU serveri kustutamisega või varem, kui projekti eesmärgid saavutatakse varem. Andmete kustutamise protsessi käigus kustutatakse ka kõik andmete varukoopiad.

Kui uuringu käigus tekib põhjendatud vajadus andmete andjalt saadud pseudonüümitud andmeid säilitada kauem, esitatakse enne uuringu lõppu eetikakomiteele vastavasisuline taotlus. Kõige tõenäolisem põhjus või vajadus võiks olla seotud teaduspublikatsioonide avaldamise pika tsükliga, kui artikli eelretsenseerimine on pooleli ja/või nõutakse täiendavaid analüüse sama andmestiku pealt.

Andmete kustutamist teostab Teadusarvutuse keskuse meeskond koostöös vastutava uurijaga, et tagada permanentne ja pöördumatu andmete kustutamine.

Andmete kustutamine dokumenteeritakse ja andmete kustutamise kohta koostatakse andmete kustutamise akt.

# Isikuandmete töötlemise eesmärgid

## Töötlemise eesmärgid

Andmete töötlemise eesmärgiks on teadustegevus, täpsemalt teadussuuringu läbiviimine: **Epilepsia epidemioloogia Eestis ja masinõppe kasutamise võimalused epilepsia epidemioloogilistes uuringutes.** Uuringi läbimiimise on heaks kiitnudEesti bioeetika ja inimuuringute nõukogu 20.08.2024. Otsus nr 1.1-12/2060.

## Töötlemise õiguslikud alused

Euroopa isikuandmete kaitse üldmääruse (2016/679, edaspidi GDPR) artikkel 9 lg 2 (j) kohaselt on lubatud töödelda eriliiki terviseandmeid s.h terviseandmeid, kui *“töötlemine on vajalik avalikes huvides toimuval teaduseesmärgil /…/, ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ning tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks.”* Alljärgnevalt on selgitatud, kuidas need nõuded on täidetud.

### Kas antud juhul toimub töötlemine teaduse eesmärgil?

Jah, andmeid töödeldakse ainult teaduse eesmärgil, täpsemalt teadusuuringute läbiviimise eesmärgil (vt eespool).

### Kas antud juhul on töötlemine vajalik avalikes huvides?

GDPR preambula p 45 kohaselt *“kui /…./ töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks /…/, peaks töötlemise alus olema sätestatud liidu või liikmesriigi õigusaktis.”* Antud juhul tuleneb liikmesriigi (Eesti) õiguslik alus järgnevast:

* Eesti isikuandmete kaitse seadus (IKS) § 6 lg 4 lubab töödelda isikuandmeid teadusuuringu vajadusteks, kui IKS nõuete tingimuste täitmist kontrollib asjaomase valdkonna eetikakomitee. Vastav komitee on Eesti bioeetika ja inimõiguste nõukogu (EBIN) näol loodud sotsiaalministri määrusega 24.09.2019 nr 60 *“Uuringueetika komitee moodustamine, selle töökord, liikmete arv ja määramise kord ning uuringu taotluse läbivaatamise tasumäärad”*. EBIN ülesandeks on (§ 3 lk 3) *“isikute põhiõiguste ennetava kaitse tagamine ja uuringutele rakendatavate hindamispõhimõtete ühtlustamine, et kindlustada uuritavate isikute õiguste kaitsemeetmed ning uurijate kohustused neid kaitsemeetmeid järgida.”* Uuringumeeskond on esitanud EBIN-le vastavasisulise taotluse ja saanud uuringu teostamiseks loa 20.08.2024 (otsus nr 1.1-12/2060).
* Tartu Ülikool on avalik-õiguslik juriidiline isik ning pakub teadustegevusel põhinevaid avalikke teenuseid. Eesti rahvast uurivate teaduste edendamine ning koostöö teiste ülikoolide ja kogu ühiskonnaga on Tartu Ülikooli seadusest tulenev Tartu Ülikooli eesmärk (Tartu Ülikooli seadus § 2 lg 2 ja 3). Taotletava eesti rahvastikul põhineva andmestiku loomise ja sellel läbiviidavate uuringutega edendab Tartu Ülikool nii meditsiini- kui andmeteadust, samuti koostööd teiste ülikoolide ja ühiskonnaga laiemalt. Tartu Ülikool teeb koostööd kogu ühiskonnaga, toetades Eesti ühiskonna arengut ja loob teadustegevusel põhinevaid võimalusi rahvusvaheliseks koostööks (Tartu Ülikooli seadus § 2 lg 5).

Seega on töötlemine vajalik avalikes huvides ning on sätestatud Eesti õiguses.

### Kas isikuandmete töötlemise ulatus on proportsionaalne saavutatava eesmärgiga?

Alljärgnevalt põhjendame, miks on vajalik just sellise suurusega andmestik, millistest andmekogudest ja milliste andmeväljade ulatuses infot kasutada soovitakse ning miks väiksem andmete ulatus muudaks kvaliteetsete terviseuuringute läbiviimise võimatuks, samuti näitame, kuidas on valitud taotletavate andmete ajavahemik ja miks on ajaliselt väiksema ajaakna andmed ebapiisavad.

Tegemist on epilepsia levimus- ja haigestumusuuringuga. Selleks, et kindlaks teha, kas tegemist on epilepsiaga või mitte, mis on epilepsia liik (fokaalne/generaliseerunud), mis on epilepsia etioloogia, millal esinesid epileptilised hood, kas patsient võtab epilepsiaravimeid, on vaja läbi vaadata iga patsiendi meditsiinilist dokumentatsiooni, s.t potentsiaalselt epilepsiaga seotud diagnoosidega ambulatoorsed ja statsionaarsed epikriisid, perearstide sissekandeid, kiirabi epikriisid jms. Vajalikud on kindlasti ka tekstilised andmed, sest ilma tekstilisi osi vaatamata on võimatu adekvaatselt hinnata, kas patsiendil on ka tegelikult epilepsia või mitte. Samal põhjusel on võimatu ehitada masinõppemudelit, mis epilepsiat võimaldaks tekstiandmete põhjal ennustada. See põhjendab, miks käesolevas uuringus on tarvis valimi kohta sellises ulatuses infot, s.h vabatekstilisi andmeid.

Käesolevas uuringus selgitatakse välja epilepsia haigestumus- ja levimusnäitajad Tartu täiskasvanud rahvastikus ning võrreldakse seda 27 aastat tagasi tehtud uuringuga. Seetõttu uuritakse käesolevas uuringus potentsiaalselt epilepsia kahtlusega patsiente Tartus (aluseks epilepsiaga seotud diagnoosikood), keda on umbes 4000 ning selgitatakse med. dokumentatsiooni läbi vaadates välja, kes neist tegelikult epilepsiat põeb (eelduslikult ca 500-600). Tartu piirkonna tuvastamiseks ja levimuse määratlemiseks küsitakse Rahvastikuregistrist elukoha andmeid. Tegemist on väga suure tööga, mille kogu Eesti ulatuses tegemine poleks mõeldav. Seetõttu uuritakse käesoleva uuringu raames võimalust teha seda tööd ära masinõppe abil, et muuhulgas hinnata kogu Eesti rahvastiku epilepsia haigestumust ja levimust. Tartu andmete märgenduste abil treenitakse masinõppemudel, et terve Eesti andmete põhjal tuvastada sealt tegelikke epileptikuid. Masinõppe mudelitele on omane, et treenimiseks ja valideerimiseks on vaja väga palju andmeid, seetõttu on selles uuringus vaja treenimiseks kogu Tartu piirkonna andmeid ning Eesti levimuse- ja haigestumuse hindamiseks kogu Eesti epilepsiakahtlusega inimeste andmeid.

Uuringumeeskonnale ei väljastata patsientide isikuandmeid. Kuigi vabatekstilistes osades võib isikuandmeid sisalduda, maandatakse seda riski anonüümimisrakenduse kasutamisega, mis eemaldab tekstidest isiku otsest tuvastamist võimaldavad tunnused.

### Kas isikuandmete töötlemine austab isikuandmete töötlemine isikuandmete kaitse õiguse olemust?

Meie hinnangul austab selles mõjuhinnangus kirjeldatud isikuandmete töötlemine isikuandmete kaitse õiguse olemust.

Võrdse kohtlemise printsiip – kirjeldatud isikuandmete töötlemine ei diskrimineeri kedagi rahvuse, soo, vanuse ega muu kuuluvuse alusel. Kõikide ühiskonna- ja vanusegruppide puhul on eesmärk toetada elukvaliteedi parandamist ja tervena elatud aastate arvu suurendamist.

Heategemise printsiip – antud andmestikust ja sellel läbiviidavatest terviseuuringutest saadav kasu on uuritavatele pigem kaudne, kuna alustatakse baasteadmiste loomisega ja otsene kliinilises praktikas kasutatav kasu haigusega tegelemiseks võib tekkida alles mitme aasta pärast. Seega saavad antud tööst kasu pigem tulevased patsiendid.

Kahju vältimise printsiip – kirjeldatud isikuandmete töötlemine on kooskõlas mittekahjustamise printsiibiga, kuna ei koorma patsiente ega põhjusta riske nende tervisele.

Taotluses kirjeldatud Uurimisgrupil on varasem kogemus sarnaste andmestike loomisel, terviseuuringute läbiviimisel ja tulemuste publitseerimisel, samuti selle valdkonna üliõpilaste õpetamisel. Uurimisgrupp on andmete töötlemiseks kirjutanud põhjaliku taotluse ja käesoleva andmekaitsealase mõjuhinnangu koos riskide maandusmeetmetega ning palunud taotlust hinnata Eesti bioeetika ja inimuuringute nõukogul ja Tartu Ülikooli inimuuringute eetika komiteel.

### Kas tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks?

Meie hinnangul on tagatud sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks.

GDPR artikkel 6 lg 4 kohaselt võtab vastutav töötleja, juhul kui isikuandmete töötlemine toimub muul eesmärgil kui andmesubjekti nõusolekul ega põhine andmesubjekti nõusolekul, arvesse m.h *“asjakohaste kaitsemeetmete olemasolu, milleks võivad olla näiteks /…/ pseudonümiseerimine”*. Artikkel 89 lg 1 kohaselt kohaldatakse avalikes huvides toimuva teaduse eesmärgil isikuandmete töötlemise suhtes andmesubjekti õiguste ja vabaduste kaitseks asjakohaseid kaitsemeetmeid. *“Need meetmed võivad hõlmata pseudonümiseerimist, kui kõnealuseid eesmärke on võimalik saavutada sellisel viisil,”* kuid nõuab vajadusel täiendavat töötlemist, kui andmesubjektid on jätkuvalt tuvastatavad (*“kui kõnealuseid eesmärke saab täita täiendava töötlemisega, mis ei võimalda või ei võimalda enam andmesubjektide tuvastamist, täidetakse need eesmärgid sel viisil.”*). Vastavad tingimused ja kaitsemeetmed tuleb preambula p 157 kohaselt sätestada liikmesriigi õiguses (*“Teadusuuringute hõlbustamiseks võib isikuandmeid töödelda teadusuuringute eesmärgil, mille suhtes kohaldatakse asjakohaseid tingimusi ja kaitsemeetmeid, mis on sätestatud liidu või liikmesriigi õiguses.”).* Eestis reguleerib isikuandmete kaitset isikuandmete kaitse seadus (IKS), mis lubab isikuandmeid andmesubjekti nõusolekuta teadusuuringu vajadusteks töödelda pseudonüümitult (IKS § 6 lg 1 *“Isikuandmeid võib andmesubjekti nõusolekuta teadus- või ajaloouuringu või riikliku statistika vajadusteks töödelda eelkõige pseudonüümitud või samaväärset andmekaitse taset võimaldaval kujul. Enne isikuandmete üleandmist teadus- või ajaloouuringu või riikliku statistika vajadustel töötlemiseks asendatakse isikuandmed pseudonüümitud või samaväärset andmekaitse taset võimaldaval kujul andmetega.”*). IKS § 6 lg 3 kohaselt on teadusuuringu vajadusteks lubatud kasutada andmeid ka andmesubjekti tuvastamist võimaldaval kujul, kui täidetud on kolm tingimust: (1) pärast tuvastamist võimaldavate andmete eemaldamist ei ole andmetöötluse eesmärgid enam saavutatavad või neid oleks ebamõistlikult raske saavutada; (2) selleks on ülekaalukas avalik huvi; (3) töödeldavate isikuandmete põhjal ei muudeta andmesubjekti kohustuste mahtu ega kahjustata muul viisil ülemäära andmesubjekti õigusi. Tervise infosüsteemi andmete kasutamist teaduse vajaduseks lubab Tervishoiuteenuste korraldamise seadus § 593 lg 7, kui vajalikkust ja põhjendust ning isikute põhiõiguste kaitsemeetmeid on hinnanud uuringueetika komitee (§ 594 lg 1 ja lg 2). Vastav komitee on EBIN näol loodud sotsiaalministri määrusega 24.09.2019 nr 60 *“Uuringueetika komitee moodustamine, selle töökord, liikmete arv ja määramise kord ning uuringu taotluse läbivaatamise tasumäärad”*. EBIN ülesandeks on (§ 3 lk 3) *“isikute põhiõiguste ennetava kaitse tagamine ja uuringutele rakendatavate hindamispõhimõtete ühtlustamine, et kindlustada uuritavate isikute õiguste kaitsemeetmed ning uurijate kohustused neid kaitsemeetmeid järgida.”*

Käesolevas projektis töödeldakse andmeid pseudonüümitud kujul, kuid lisaks rakendatakse andmesubjektide tuvastamise riski maandamiseks ka täiendavat töötlust:

1. Taotletav andmestik ei sisalda isikute nimesid, isikukoode, aadresse jms. Taotletavad andmed pseudonüümitakse andmeallikate poolt enne Uurimisgrupile väljastamist. Pseudonüümimisvõti on tagasipööramatu ning seda taotluses kirjeldatud meeskonnale ei avaldata.
2. Andmestiku loomisel ega hiljem ei toimu depseudonüümimist ja uuritavatega ühendust ei võeta.
3. Uurimismeeskond tagab tehnilisi ja korralduslikke meetmeid rakendades täiendava kontrolli saadud andmestikule võimalilke isikuandmete tuvastamiseks ja nende olemasolul nende eemaldamiseks
4. Andmete töötlus toimub spetsiaalsel tundlike andmete platvormil SAPU, mis piirab kasutajate võimalust andmeid serverist välja kopeerida ega võimalda andmeid muul moel linkida teiste andmestikega (maandab linkimisründe riski andmesubjektide tuvastamiseks).
5. Esimeseks tegevuseks SAPU serveris on andmete töötlemine automaatse anonüümimisrakendusega, et eemaldada andmete vabatekstilistest osadest võimalikud nimed, telefoninumbrid, isikukoodid, aadressid.

Muud kaitsemeetmed on kirjeldatud käesoleva mõjuhinnangu lõpus.

Kuigi käesolevas uuringus ei kasutata andmeid andmesubjekti tuvastamist võimaldaval kujul, vaid pseudonüümitult ja rakendatakse ka muid kaitsemeetmeid andmesubjekti tuvastamise riski maandamiseks, on siiski täidetud ka IKS § 6 lg 3 kolm tingimust: (1) terviseuuringute, s.h ravijärgimuse ja ravitrajektooride uurimiseesmärke oleks ebamõistlikult raske saavutada ilma üksikpatsientide tasemel andmeid analüüsimata; (2) uuringu vastu on ülekaalukas avalik huvi (vt põhjendust eespool); (3) töödeldavate isikuandmete põhjal ei muudeta andmesubjekti kohustuste mahtu ega kahjustata muul viisil ülemäära andmesubjekti õigusi (samuti põhjendatud eespool).

# Riskid ja nende maandamine

Riskide kaardistus koos maandamise meetmega on toodud järgmises tabelis. Riski tõenäosust on hinnatud pärast maandusmeetmete rakendamist (nt ilma SAPU kasutamiseta oleks tõenäosused märgatavalt suuremad):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Riski nr** | **Riski nimetus** | **Jääkriski tõenäosus**  **(0-väga madal; 4-väga kõrge)** | **Riski mõju (0-väga madal; 4-väga kõrge)** | **Riski tase** | **Tegevused / ettepanekud riski maandamiseks** |
| 1 | Inimeste terviseandmed saavad avalikuks | 1 (madal) | 4 (väga kõrge) | Keskmine | SAPU kasutamine (ei saa kopeerida), mis on kättesaadav vaid Tartu Ülikooli sisevõrgust ainult Uurimisgrupi liikmetele, serveri monitooring ja tegevuste logimine, kindel protsess andmete SAPU-st väljatoomiseks, pika kogemusega Uurimisgrupi liikmed, konfidentsiaalsusklausel töölepingus, füüsilised turvameetmed serveriruumil, andmed pseudonüümitud. Uurimisgrupi liikmete juhendamine ja koolitamine. |
| 2 | Andmestikus olevate andmesubjektide suurel hulgal (süstemaatiline) tuvastamine | 1 (madal) | 4 (väga kõrge) | Keskmine | Otseste isikuandmete eemaldamine andmealliakte poolel enne Uurimisgrupile edastamist, unikaalsete pseudonüümide kasutamine, SAPU kasutamine (ei saa andmeid kopeerida ega teiste andmestikega linkida) |
| 3 | Andmestikus konkreetse andmesubjekti juhuslik tuvastamine | 2 (keskmine) | 2 (keskmine) | Keskmine | Otseste isikuandmete eemaldamine andmeallikate poolel enne Uurimisgrupile edastamist, unikaalsete pseudonüümide kasutamine. Säilib risk, et mõni patsient on arstidest uurimismeeskonna liikmetele läbi isikliku praktika ja haiguloo tuttav ning seeläbi äratuntav, ning seeläbi saadakse patsientide kohta ka uut informatsiooni. Riski maandamiseks on selliste uurijate hulk käesolevas uuringus piiratud, andmed saadakse üksnes epilepsiaga seotud tervisedokumentide kohta, toimub serveri monitooring ja tegevuste logimine (s.h ekraanivideo), kindel protsess andmete SAPU-st väljatoomiseks. |
| 4 | Andmestikust iseenda tuvastamine | 3 (kõrge) | 0 (väga madal) | Keskmine | Otseste isikuandmete eemaldamine enne Uurimisgrupile edastamist, unikaalsete pseudonüümide kasutamine, iseenda tuvastamisel ei saa uurija teada uut informatsiooni |
| 5 | Andmeallikad avaldavad Uurimisgrupile pseudonüümimis-parooli, mis muudab andmesubjektid Uurimisgrupi poolt tuvastatavaks | 1 (madal) | 2 (keskmine) | Keskmine | Selgelt kindlaksmääratud protsess parooli vahetamiseks andmeallikate vahel ilma seda Uurimisgrupile avaldamata, SAPU kasutamine (ei saa andmeid kopeerida ega teiste andmestikega linkida) |
| 6 | Vabatekstiline info võib sisaldada sensitiivseid andmeid | 2 (keskmine) | 1 (madal) | Keskmine | Andmete saamisel on SAPU serveris esimeseks sammuks anonüümimisrakenduse kasutamine, mis tuvastab ja asendab vabatekstilistes dokumendiosades isikunimed, aadressid, telefoninumbrid, isikukoodid. Juhuleidude korral on Uurimisgrupil kindel protsess nende käsitlemiseks, täiendatakse vastavalt anonüümimisrakendust ja teostatakse anonüümimine uuesti. |
| 7 | Andmetele saavad ligi Uurimisgrupi välised isikud | 2 (keskmine) | 1 (madal) | Keskmine | SAPU serverisse kasutajakontode lisamine ja eemaldamine käib kindlaksmääratud protsessi alusel, regulaarselt vaadatakse üle kõigi kasutajate õigused, lähtutakse TÜ IT-turbe kordadest ja kõik Uurimisgrupi liikmed peavad läbima küberhügieeni ja kodust töötamise infoturbe alased ning andmekaitse alse koolitused ja eksamid (<https://cyberhygiene.ut.ee/>) |
| 8 | Andmeid kasutatakse uurimismeeskonna poolt muuks otstarbeks kui lubatud | 1 (madal) | 1 (madal) | Madal | SAPU kasutamine (ei saa andmeid kopeerida, automaatne tegevuste logimine), Uurimisgrupi kõrge kvalifikatsioon ja pikaaegne kogemus terviseandmetega töötamisel |
| 9 | Avaldatavad tulemused on liiga detailsed (andmesubjektide tuvastamise risk) | 1 (madal) | 1 (madal) | Madal | Kindel protsess andmete SAPU-st väljatoomiseks, tulemuste avaldamisel kontrollitakse, et tagatud on k>=5 anonüümsus, pika kogemusega Uurimisgrupi liikmed |

# Kasutusel olevad riskide vältimise meetmed

Tartu Ülikoolis on riskide vältimise aluseks riskianalüüs, mida tehakse igas vajalikus valdkonnas / teemas / projektis ning selle eest on vastutav vastava valdkonna / teema / projekti esindaja.

Riskianalüüsi käigus:

* kirjeldatakse võimalikud riskid,
* hinnatakse iga riski tõenäosust ja võimalikku mõju,
* vastavalt riski tõenäosusele ja võimalikult mõjule määratakse riski tase,
* vajadusel kirjeldatakse riskide kontrollimise ja maandamise tegevused.

Regulaarseid riskianalüüse viiakse läbi vastavalt vajadusele.

Antud projektis vastutab riskide vältimise ja vajalike meetmete rakendamise eest vastutav uurija, kes saab vajadusel abi Tartu Ülikooli siseauditi büroolt.

## Füüsilised turvameetmed

Andmetöötlus toimub Tartu Ülikooli teadusarvutuste keskuse infrastruktuuril:

* Jälgitakse Eesti infoturbestandardiga kehtestatud nõudeid.
* Erinevad ressursid on eraldatud võrgu tasandil.
* Töötajaid koolitatakse järjepidevalt.
* Kõik võrguseadmed ja serverid asuvad Tartu Ülikooli majutatud suletud andmekeskustes.
* Andmekeskustes kasutatavad tulekustutussüsteemid toimivad automaatselt, on gaasipõhise lahendusena ning on ette nähtud andmekeskustes kasutamiseks.
* Andmekeskustes ei hoita kergestisüttivaid või tuleohtlikke esemeid.
* Andmekeskuste konstruktsioonides ja sisustuses on viidud miinimumini süttivate materjalide, nagu puu, tekstiil ja sünteetilised materjalid kasutamine.
* Andmekeskused on kaitstud uputuste ja veekahjustuste eest.
* Andmekeskustes on tagatud optimaalne temperatuur ja õhuniiskus.
* Andmekeskused on kaitstud sissemurdmise ja volitamata sisenemise eest.
* Füüsiliselt pääsevad andmekeskusesse nimelist (personaalset) juurdepääsuõigust omavad isikud.
* Isikliku juurdepääsuõigusega isikud pääsevad andmekeskusesse kas võtme või töötõendi ja valvekoodi abil.
* Ilma isikliku juurdepääsuõiguseta isikutel on võimalik andmekeskusesse siseneda üksnes andmekeskusesse juurdepääsu omava isiku juuresolekul.
* Andmekeskuste turvalisuse tagamiseks kasutatakse tehnilist valve- ja läbipääsusüsteemi ning videovalvet.
* Valve- ja läbipääsusüsteem salvestab andmed juurdepääsukaartide kasutamise ja valvestamise kohta.
* Andmekeskused asuva kahe tulekindla ukse taga, mida saab avada vaid isikliku kiipkaardiga või spetsiaalse võtmega.
* Andmekeskused on elektroonilise valve all ning andmekeskusesse sisenemisel tuleb elektrooniline valve isikliku koodi abil deaktiveerida.
* Andmekeskuse elektrooniline valve on deaktiveeritud ainult siis, kui keegi asub füüsiliselt andmekeskuses, on sinna sisenemas või sealt lahkumas.
* Kõik andmekeskusse sisenemised ja elektroonilise valve deaktiveerimised/aktiveerimised logitakse.
* Tuleohutuse tagamisel järgitakse Ülikooli tuleohutuseeskirju.
* Tartu Ülikooli teadusarvutuste keskuses kehtivad tehnilised ja organisatoorsed meetmed infoturbe tagamiseks ning andmete kaitsmiseks. Valik tehnilisi ja organisatoorseid meetmeid (turvakaalutlustel ei ole avalikustatud kõik tehnilised ja organisatoorsed meetmed) on toodud Tartu Ülikooli teadusarvutuste keskuse koduleheküljel <https://hpc.ut.ee/terms/information-security> (inglise keeles).

## Infotehnoloogilised turvameetmed

Andmetöötlus toimub Tartu Ülikooli teadusarvutuste keskuse infrastruktuuril SAPU keskkonnas, kus:

* Jälgitakse Eesti infoturbestandardiga kehtestatud nõudeid.
* Teostatakse regulaarselt serverite testimist, uuendamist ja monitoorimist.
* Haavatavuste tuvastamiseks kasutatakse monitoorimist, masinõpet ning ka erinevaid läbistusteste. Muuhulgas kasutatakse haavatavuste tuvastamiseks ka juba olemasolevaid haavatavuste tuvastamise tarkvarasid (näiteks Nessus) ning jälgitakse järjepidevalt erinevaid haavatavuste nimekirju. Lisaks Tartu Ülikooli teadusarvutuste keskusele skaneerib Tartu Ülikooli teadusarvutuste keskuse avalikult kättesaadavaid ressursse ka CERT-EE.
* Erinevad ressursid on eraldatud kasutajaõiguste tasandil.
* Õiguste määramisel lähtutakse minimaalsuse põhimõttest ja vaikimisi administraatori juurdepääsu ei võimaldata.
* Servereid skaneeritakse regulaarselt ja jooksvalt jälgitakse ka võrguliiklust.
* Vaikimisi on keelatud kõik tegevused, mis ei ole otseselt vajalikud töö tegemiseks.
* Kasutatakse andmete varundamist Tartu Ülikooli teadusarvutuste keskuse lindirobotile, mis asub füüsiliselt teises asukohas (Tartu Ülikooli teadusarvutuste keskuse andmekeskuses).
* Kõik kasutajate tegevused SAPU keskkonnas logitakse.
* Kõik potentsiaalsed turvaintsidendid ja turvanõrkuste leidmise katsed logitakse (näiteks sisse logimise katsed, pöördumised erinevate portide poole, kasutajaõiguste muutused jne).
* SAPU keskkonnas olevate kasutajate ekraanipilt salvestatakse.
* SAPU keskkonnast info/andmete välja liigutamine on võimalik ainult, kui vastutav uurija on vastavad andmed üle vaadanud ja selleks nõusoleku andnud.
* SAPU keskkonnast info/andmete välja kopeerimine ei ole võimalik („copy“ käsk).
* SAPU keskkond asub eraldi tulemüüri taga.
* Interneti juurdepääs SAPU masinast on täielikult suletud ja ei ole võimalik teha päringuid internetti.
* SAPU keskkonnas on eelinstalleeritud tarkvara ja kasutajal ei ole võimalik keskkonda tarkvara ise installeerida.
* Andmete liigutamine (kaasa arvatud analüüsi tulemuste) SAPU keskkonnast välja vajab kolmanda isiku (andmete omaniku) nõusolekut.
* SAPU keskkondi varundatakse regulaarselt.
* Perioodidel, kui SAPU keskkonda ei kasutata, on keskkond välja lülitatud ja keskkonda ei ole võimalik siseneda.
* Tartu Ülikooli teadusarvutuste keskuses kehtivad tehnilised ja organisatoorsed meetmed infoturbe tagamiseks ning andmete kaitsmiseks. Valik tehnilisi ja organisatoorseid meetmeid (turvakaalutlustel ei ole avalikustatud kõik tehnilised ja organisatoorsed meetmed) on toodud Tartu Ülikooli teadusarvutuste keskuse koduleheküljel <https://hpc.ut.ee/terms/information-security> (inglise keeles).