|  |  |
| --- | --- |
|  | /\*ASUTUSESISESEKS KASUTAMISEKS  Märge tehtud: 05.01.2024  Kehtib kuni: 05.01.2029  Alus: AvTS § 35 lg 2 p 3  Teabevaldaja: Sotsiaalministeerium\*/ |
| **Sotsiaalministeeriumi sotsiaal- ja töövaldkonna uuringute ja analüüside ajutise eetikakomitee elektroonilise koosoleku protokoll nr 14** | 05.01.2024 |

Juhatas: Kristi Rüütel

Protokollis: Marion Pajumets

Võtsid osa: Rein Murakas, Marge Unt

Puudus(id): –

Kutsutud: Rein Murakas, Marge Unt, Kristi Rüütel

Koosolek toimus ajavahemikus 04.12.2023 – 28.12.2023 e-kirjade teel.

**PÄEVAKORD:**

1. Hinnang taotlusele "Lasteabitelefoni 116 111 tulemuslikkuse uuring".

Eetikakomitee hindas taotlust, mis oli esitatud Andmekaitse Inspektsiooni vormil ning palus taotlejal esitada asjakohaseid dokumente. Lisaks esitas eetikakomitee taotlejale lisaküsimusi ning sai neile vastuseid, mis on toodud protokolli Lisas 1.

**OTSUSTATI:**

1.1. Eetikakomitee annab 28.12.2023. a kooskõlastuse uuringu "Lasteabitelefoni 116 111 tulemuslikkuse uuring " läbiviimiseks.

**Lisa 1. Taotluse läbivaatamisel tekkinud küsimused-vastused ja soovitused Sotsiaalministeeriumi sotsiaal- ja töövaldkonna uuringute ja analüüside ajutiselt eetikakomiteelt**

*(allkirjastatud digitaalselt)* *(allkirjastatud digitaalselt)*

Kristi Rüütel Marion Pajumets

Koosoleku juhataja Protokollija

**Lisa 1. Taotluse läbivaatamisel tekkinud küsimused-vastused ja soovitused Sotsiaalministeeriumi sotsiaal- ja töövaldkonna uuringute ja analüüside ajutiselt eetikakomiteelt**

1. **ring küsimusi-vastuseid**
   1. **Küsimus:** Kas STAR keskkonda sisestatud info hõlmab ka olukorra kirjelduse ja toimingud? Töödeldavate isikuandmete koosseis jääb mulle kui teemavälisele isikule segaseks. Mainitakse järgmist: „menetlused, pöördumised, toimingud ja rakendatud abinõud. Lapse lastekaitsealaste juhtumiplaanide väljavõtted“ See ei saa ju olla Excel tabel, vaid pigem mingid kirjeldused ja sõnalised kokkuvõtted?
   2. **Vastus:** STAR keskkonda sisestatud info hõlmab ka olukorra kirjeldust ja toiminguid. Põhjaliku ülevaate töödeldavate andmete koosseisust annab 15.12.2023 esitatud AKI täiendatud taotluse lisa 3. Väljavõte STAR-ist tehakse SQL programmi kasutades ning väljavõte on exceli tabeli kujul, kus iga andmeväli on eraldi veeruna. STAR kasutaja (lasteabi nõustaja, lastekaitsetöötaja) täidab nii etteantud valikutega kui ka vabavälju, lisaks genereeritakse süsteemsed pöördumised (nt „Pöördumise registreerimine“, „Juhtumimenetluse algatamine“) ning sellest olenevad ka vastavate lahtrite sisud väljavõttes. Kokku tekib mitu erinevat andmetabelit, mis unikaalse pseudonümiseeritud isikukoodi ja/või menetluse numbri abil annavad tervikliku vaate juhtumist.
   3. **Küsimus:** Mainitakse pseudonüümimist: „Laste delikaatsed isikuandmed (isikukood, täpne elukoht, lapse ja pere nimed) pseudonümiseeritakse, et võimaldada küll seoste loomist, ent mitte laste ära tundmist.“ Mida see reaalselt tähendab? Pseudonüümimise puhul tekib koodi võti, et oleks hiljem võimalik isik tuvastada. Kuidas pseudonüümitakse? Kes need inimesed STARis on, kes kõik need pikad tekstid läbi töötavad ja teevad kindlaks, et selles ei ole mingeid tunnuseid, mis viitaksid isikutele? Kus ja kui kaua säilitatakse koodi võtit, kellele on sellele ligipääs?
   4. **Vastus:** Pseudonümiseerimist on kirjeldatud 15.12.23 AKI-le esitatud täiendatud taotluses. Pseudonümiseerimisel lähtutakse Euroopa Liidu Küberturvalisuse Ameti (ENISA) juhendist[[1]](#footnote-1) pseudonüümimisvõtete ja parimate tavade kohta. Pseudonümiseerimiseks kasutatakse exceli valemit, mille on loonud andmehaldus talituse analüütik. Isikukoodis antakse igale numbrile uus alfabeetiline väärtus. Erinev number isikukoodis võib olla asendatud sama tähega, mistõttu ei ole võimalik koodi murda ja valemi abil tagasipöörata. Pseudonümiseerimise võtit (isikukoodide ja pseudonüümide vastavustabel) säilitatakse turvatud võrgukettal piiratud ligipääsuga kaustas vastavalt andmekogude säilitamise tähtajaga, mis on maksimaalselt kuni 2024 IV kvartalini. Isikuandmed (nt nimi ja perekonnanimi, isikukood, täpne aadress, telefoninumber, e-posti aadress, ID-kaardi vms dokumendi number jm) pseudonümiseeritakse (või kustutatakse, kui andmed ei ole uuringu vaates olulised) vastutava töötleja (Sotsiaalkindlustusamet) andmehaldustalituse analüütiku ning ennetustalituse peaspetsialisti poolt valemite abil. Samade töötlejate poolt loetakse täiendavalt üle ka vabaväljadel olev tekst, et välistada isikute kaudset tuvastamist (nt kool ja klass). Volitatud töötlejale (AS Emor) edastatakse pseudonümiseeritud andmed.
   5. **Küsimus:** Kirjutatud on „Emoril kohustus uuringu käigus kogutud andmekogud säilitada kodeerituna ja hulgana, mis välistab nende samastamise konkreetsete isikutega, välja arvatud kui kokkuleppel tellijaga otsustatakse andmekogus olevad andmed (osaliselt või tervikuna) hävitada“ Samas on eespool kirjutatud: „Taotleja (Sotsiaalkindlustusamet) teeb andmetest väljavõtu, pseudonümiseerib andmed ja edastab need krüpteeritult ja kasutades turvalist vahenduskeskkonda uuringu läbiviija kontaktile ehk Kantar Emori (volitatud töötleja) töötajale.“ Kui SKA pseudonüümib, kuidas siis saab nõuda veel Emorilt, et nemad peavad tagama selle, et pole võimalik samastada konkreetse isikuga?
   6. **Vastus:** Kuigi isiku otsest tuvastamist võimaldavad andmed pseudonümiseeritakse, siis eelkõige süvaanalüüsi hõlmatud juhtumite puhul võib esineda asjaolusid, mis kaudselt, eri andmetest kombineerituna, võivad võimaldada seoste loomist konkreetsete isikutega. Seetõttu on vajalikud ka töövõtulepingus ning töövõtulepingu lisas 1 (andmetöötluse leping) toodud tingimused andmete töötlemise ja andmekogude säilitamise osas. Ka IKS-i[[2]](#footnote-2) § 6 lg 1 kohaselt võib teadusuuringu eesmärgil ilma inimese nõusolekuta tema isikuandmeid töödelda vaid pseudonüümitult või samaväärset kaitset võimaldaval kujul. Kättesaadavates juhendimaterjalides pseudonümiseerimise osas, nt Tallinna Ülikooli andmekaitse juhendis[[3]](#footnote-3) tuuakse välja, et „Üldmääruse kohaselt on pseudonüümimine isikuandmete töötlemine selliselt, et isiku tuvastamist võimaldavad andmed on eemaldatud ja asendatud pseudonüümiga, näiteks koodi või muu tunnusega. Sellised andmed on siiski isikuandmed ja nende töötlemisel tuleb järgida andmekaitse põhimõtteid. Pseudonüümimine on lisanduv kaitsemeede, millega kaitstakse andmesubjekti õigusi, kuid ei vabasta teadlast vastutusest andmekaitse nõuete järgimise eest.“
   7. **Küsimus:** Mida tähendab, et välja arvatud kui otsustakse andmed hävitada? Kas on siis võimalus, et neid säilitatakse igavesti? Kus ja miks? Isikuandmeid peaks töötlema vaid niikaua, kui see on hädapäraselt vajalik, ning ka anonüümsete andmete säilitamine igavesti volitatud töötleja poolt ei tundu põhjendatud. Hiljem on kirjutatud: „Töövõtja krüpteerib vastavad andmekogud hiljemalt kahe kuu jooksul pärast tööde üleandmist tellijale, mida töövõtja kinnitab allkirjaga eraldi aktil. Krüpteeritud andmekogu säilitamise tähtaja ja tingimused lepivad pooled kokku valmis töö üleandmisel. Seda seetõttu, et sel hetkel võib olla täiendavaid kaalutlusi andmete säilitamise aja osas (nt teadustöö, kvaliteedikontroll vms), kuid maksimaalne andmete säilitamise tähtaeg on kuni kaks aastat peale töö üleandmist.“
   8. **Vastus:** AS Emoriga sõlmitud lepingu nr 5.2-9/3598- 1 punktis 9.7 on kokkulepitud, et: “Töövõtjal on kohustus uuringu käigus kogutud andmekogud säilitada kodeerituna ja hulgana, mis välistab nende samastamise konkreetsete isikutega, välja arvatud kui kokkuleppel tellijaga otsustatakse andmekogus olevad andmed (osaliselt või tervikuna) hävitada.“ See tähendab, et võib esineda kaalutlusi, mistõttu otsustatakse näiteks süvaanalüüsi hõlmatud andmekogud (juhtumiplaanid) hävitada neis sisalduvate juhtumite kirjelduste detailsusastme tõttu, samas laias valimis olevad pseudonümiseeritud andmekogude säilitamine võib olla vajalik vastutavale töötlejale täiendava kvaliteedikontrolli jaoks. AKI-le esitatud täiendatud taotluses on täiendavalt selgitatud andmete säilitamist ja määratud konkreetsem ja lühem tähtaeg: „AS Emoriga sõlmitud lepingu nr 5.2-9/3598- 1 punktis 4.1 on kokku lepitud, et lõppraporti mustandi üleandmine toimub mitte hiljem kui 10.05.2024. Ajakava on võimalik kohandada lepingu täitmise käigus eeldusel, et parandatud lõppraporti esitamine toimub hiljemalt 2024. a juuni lõpus. Andmekogu maksimaalne säilitamistähtaeg jääb 2024. aasta IV kvartalisse. Seda seetõttu, et sel hetkel võib olla täiendavaid kaalutlusi andmete säilitamise aja osas (nt teadustöö, kvaliteedikontroll vms).“
   9. **Küsimus:** Ma eeldan, et „töö“ on raport või aruanne, mis nende andmete põhjal valmib? Miks on vaja oodata kaks kuud andmete krüpteerimisega ja miks üldse peavad töövõtjale algandmed jääma? Miks peaksid need andmed nii kaua Emoris alles olema? Emorit ei pruugi kahe aasta pärast olemaski olla.
   10. **Vastus:** Volitatud töötlejale on kaks kuud andmete krüpteerimiseks ja edastamiseks, kuna tulenevalt töövõtulepingu punktist nr 5.2-9/3598- 1 punktist 4.1.2 on töövõtja kohustatud koostama esitluse ja tutvustama projekti tulemusi kokkuleppel tellijaga minimaalselt kahel tellija poolt välja pakutud üritusel kuni kahe kuu jooksul peale lõppraporti esitamist. See tähendab, et andmete krüpteerimine jääb lepinguperioodi sisse ning on põhjendatud kui peaks ilmnema vajadus andmete täiendavaks kvaliteedikontrolliks. Andmekogu maksimaalne säilitamistähtaeg jääb 2024. aasta IV kvartalisse.
2. **ring küsimusi-vastuseid**
   1. **Küsimus:** Üks tähelepanek. Kui „Pseudonümiseeritud andmeid ei ole võimalik uuesti isikustatud kujule viia, kuna pseudonümiseerimise käigus võivad valemi alusel isikukoodi erinevatele numbritele antud sümbolid korduda (samas on tagatud pseudonüümide unikaalsus, et eristada juhtumeid).“ siis ei ole tegemist pseudonüümimisega klassikalises mõttes, vaid lihtsalt igale uuritavale antakse unikaalne kood.
   2. **Vastus:** Pseudonümiseerimisel lähtutakse Euroopa Liidu Küberturvalisuse Ameti (ENISA) juhendist[[4]](#footnote-4) pseudonüümimisvõtete ja parimate tavade kohta, kus Lasteabi tulemuslikkuse uuringu raames andmete edastamist kirjeldab mudel 3 Pseudonümiseeritud andmete edastamine töötlejale. Vastutav andmetöötleja viib läbi pseudonümiseerimise, kuid volitatud töötlejat protsessi ei kaasata, vaid volitatud töötleja ainult võtab vastu vastutavalt töötlejalt pseudonüümseks muudetud andmed. Volitatud töötleja jaoks ei ole pseudonüümid tagasipööratavad. Ka vastutav töötleja ei saa andmeid depseudonümiseerida valemi abil, vaid pseudonüümide isikutega seostamiseks luuakse pseudonüümi võti, mida säilitatakse andmetest eraldi (võtme säilitamist on eelnevalt selgitatud küsimusele nr 2 antud vastuses). Pseudonümiseerimise tehnika aluseks on jaotises 5.2 käsitletud Random number generator (RNG), mis käsiraamatu alusel pakub tugevat andmete kaitset.
   3. **Küsimus:** Eraldi teema on see, kas kõigi loetelus olevate tunnusete abil on siiski võimalik mõnda uuritavat kaudselt tuvastada, mis tähendaks, et toimub isikuandmete töötlemine. Näiteks meile alles nüüd saadetud xls failist selgub, et päritakse lapse vanus kuu ja aasta täpsusega. Miks on vajalik kuu ja aasta, mitte lihtsalt vanus täisaastates? Kui küsitakse veel valda/Tallinna linnaosa ning surmaaega kuu ja aasta täpsusega, siis mõni väiksema piirkonna laps muutub kindlasti üheselt tuvastatavaks. Selgusetuks jääb ka „soo“ tunnuse kasutamine.
   4. **Vastus:** Esineb võimalus, et eri andmetest kombineerituna on võimalik luua seoseid konkreetsete isikutega. Seetõttu on vajalikud ka töövõtulepingus ning töövõtulepingu lisas (andmetöötluse leping) toodud tingimused andmete töötlemise ja andmekogude säilitamise osas. Kuu ja aasta täpsusega sünniaeg võimaldab volitatud töötlejal teha täpsemaid arvutusi lapse vanuse osas menetluse algatamise hetkel, mida ei võimalda lapse vanus kindla kuupäeva seisuga. Surma kuu ja aasta võimaldab paigutada ajajoonel ligikaudse surma hetke ja teha järeldusi juhtumi käigu osas (nt kas lapse perest eraldamise hetkel oli vanem elus). Aadressi täpsusastet arutasime täiendavalt uuringufirmaga ning lähtusime aadressi detailsusastme otsustamisel, et tööpraktikad linnaosade lõikes võivad oluliselt erineda ning Tallinna linnaosade elanike arv ületab Eesti väiksemate KOV-ide elanikke arvu. Selgusetuks jääb ka „soo“ tunnuse kasutamine“. Soo tunnust kasutame analüüsis ja soo tunnuse saame isikukoodist enne pseudonümiseerimist.
3. **ring küsimusi-vastuseid**
   1. **Küsimus:** Ma ei leidnud läbi vaadates selget EMOR poolset kirjeldust, kuidas nad kohustuvad andmeid hoidma - mis arvutis (kas sülearvuti, mida võetakse ka kodukontorisse?). Kui hoitakse mitmes, siis kõigi kirjeldus vajalik, kuidas tagatakse andmete hoidmise turvalisus ja  kes pääseb ligi? Eeldan, et nad on selle läbi mõelnud, aga hea oleks näha kirjapanduna (mitte viitena regulatsioonile, vaid reaalselt kuidas EMORis toimub). Seda on niikuinii vaja ka lepingu sõlmimisel selle inimesega, kes neid andmeid analüüsib.
   2. **Vastus:** Emor hoiab andmeid turvatud võrgukettal, millel on ligipääs läbi turvalise ühenduse vaid õigustatud isikutel.
   3. **Küsimus:** Pseudonüümide/koodide (heal lapsel mitu nime) teema on minu kui pidevalt juhuslike arvude generaatorit kasutaja jaoks enam-vähem OK. Andmete kustutamise teemaga ma ka edasi ei tegeleks (see on pikem teema, aga praegused algandmed on nagunii vajadusel uuesti algallikast tekitatavad), küll aga tuleks fikseerida, kuidas on ligipääs reguleeritud võimaliku edasise tegevuse (kontroll, teadustöö, vms) käigus võimalike protsessi lisanduvate isikute osas (või on  üheselt fikseeritud, et ühtegi uut isikut ei kaasata).
   4. **Vastus:** Andmeid töötlevate isikute ringi ei ole plaanis laiendada. Kui selleks peaks ilmnema vältimatu vajadus, siis tehakse seda vastavalt ettenähtud regulatsioonidele.

1. Pseudonymisation techniques and best practices (2019). European Union Agency for Cybersecurity (ENISA) file:///C:/Users/kristi.asser/Downloads/Guidelines%20on%20shaping%20technology%20according%20to%20GDPR%20provisions.pdf Kasutatud 18.12.2023 [↑](#footnote-ref-1)
2. Isikuandmete kaitse seadus [https://www.riigiteataja.ee/akt/104012019011#para6](https://www.riigiteataja.ee/akt/104012019011%23para6) Kasutatud 18.12.2021 [↑](#footnote-ref-2)
3. Pihlaks, G. (2022). Andmekaitse juhend: Isikuandmete töötlemine teadustöös (2022). Tallinna Ülikool

   <https://www.tlu.ee/sites/default/files/TUKO/veeb/failid/Andmekaitse_juhend_Isikuandmete_tootlemine_teadustoos_092022_final.pdf> Kasutatud 18.12.2021 [↑](#footnote-ref-3)
4. Pseudonymisation techniques and best practices (2019). European Union Agency for Cybersecurity (ENISA) [file:///C:/Users/kristi.asser/Downloads/Guidelines%20on%20shaping%20technology%20according%20to%20GDPR%20provisions.pdf](file:///C:\Users\kristi.asser\Downloads\Guidelines%2520on%2520shaping%2520technology%2520according%2520to%2520GDPR%2520provisions.pdf) Kasutatud 18.12.2023 [↑](#footnote-ref-4)