Andmekaitse teadustöös
Juhend

Selle juhendi eesmärk on toetada Tartu Ülikooli teadlasi hea teadustava järgimisel. Kuna see eeldab paratamatult mingil määral ka andmekaitsepõhimõtete tundmist, käsitletakse siin eetilist ümberkäimist isikuandmetega ja nende töötlemist teadustöös.

Juhendis selgitatakse, kuidas mõjutavad isikuandmete kaitsega seotud õigusnormid teadustöö tegemist ja millised on sellega seotud erandid. Juhendi lugemine ei eelda andmekaitsealaseid teadmisi: kõiki olulisi mõisteid ja üldisi põhimõtteid on selgitatud esimeses peatükis.

Edasi on juhend üles ehitatud andmete elutsükli järgi: teises peatükis käsitletakse teadustöö planeerimist, kolmandas andmete kogumist ja analüüsi ning neljandas andmete avaldamist ja säilitamist. Kui juhendis ei leidu vastust mõnele konkreetsele küsimusele, võib pöörduda Tartu Ülikooli andmekaitse spetsialistide poole e-posti aadressil admekaitse@ut.ee.

Juhendi loomine sai alguse Tartu Ülikooli eetikakeskuse korraldatud aruteludest hea teadustava ja andmekaitse kokkupuute kohtadest. Autorid tänavad kõiki, kes aruteludel osalesid või nõu ja tagasisidega juhendi loomisel abiks olid: Raul Kangro, Aime Keis, Maarja Kirss, Kairi Kreegipuu, Katrin Laas-Mikko, Kristi Lõuk, Hetel Muru, Mari-Liisa Parder, Grete Pihlakas, Kärt Pormeister, Henri Schasmin, Kadri Simm, Andres Soosaar, Margit Sutrop, Katrin Velbaum.

Juhendi valmimist toetas TÜ arengufondi projekt „Hea teadustava rakendamine ja valdkondliku nõustasmissüsteemi käivitamine“ (2020–2022).

Autorid: Marten Juurik, Terje Mäesalu, Tiiu Tarkpea.

Toimetaja: Helika Mäekivi

Sisukord

1. Andmekaitse põhimõisted 7
   1.1. Mis on isikuandmete kaitse? 7
   Andmekaitse Tartu Ülikoolis 7
   1.2. Millised on peamised isikuandmete kaitse õigusaktid? 7
   Mis muutus üldmääruse jõustumisega? 8
   1.3. Mis on isikuandmed? 9
      1.3.1. Eriliiki isikuandmed 10
      1.3.2. IP-aadressid 10
   1.4. Mis on isikuandmete töötlemine? 11
   1.5. Millised on andmekaitsepõhimõtted? 13
      1.5.1. Isikuandmete töötlemine on seaduslik ja õiglane 13
      1.5.2. Isikuandmete töötlemine on läbipaistev 13
      1.5.3. Isikuandmete töötlemine on eesmärgipärane 13
      1.5.4. Isikuandmete töötlemine on minimaalne 14
      1.5.5. Isikuandmete töötlemine põhineb kvaliteetsetel andmetel 14
      1.5.6. Isikuandmete säilitamise piirang 14
      1.5.7. Isikuandmete töötlemine on turvaline 14
      1.5.8. Lõimitud andmekaitse 15
      1.5.9. Vaikimisi andmekaitse 15
      1.5.10. Pseudonüümimine ja anonüümimine 15
   1.6. Mis on õiguslik alus? 16
   1.7. Kuidas on hea teadustava seotud isikuandmete töötlemisega? 16
2. Teadustöö planeerimine 18
   2.1. Millega alustada, kui teadustöös on kavas isikuandmeid töödelda? 18
   2.2. Kui palju peab teadustöös isikuandmetega seonduvat dokumenteerima? 20
      2.2.1. Andmehaldusplaan 20
      2.2.2. Andmekaitsetingimused 21
      2.2.3. Ülevaade isikuandmete töötlemisest 21
      2.2.4. Eetikakomitee kooskõlastus 22
      2.2.5. Andmekaitsealane mõjuhinnang 22
      2.2.6. Informeeritud nõusolek 22
   2.3. Milline peab olema inimeselt küsitav nõusolek? 23

2.3.1. Nõusolek peab olema vabatahtlik 23
2.3.2. Nõusolek peab olema teadlik 23
2.3.3. Nõusolek peab olema konkreetne ja ühemõtteline 24
2.3.4. Isikuandmete töötlemise nõusolek peab selgelt eristuma muudest nõuetest ja nõusolekutest 24
2.3.5. Nõusoleku andmist peab suutma tõendada 25
2.3.6. Töötlemine peab piirduma nõusolekus kirjeldatuga 25
2.3.7. Nõusolekut peab olema lihtne tagasi võtta 25
2.4. Mida pidada silmas, kui isikuandmeid töödeldakse ilma inimese nõusolekuta? 25
2.4.1. Andmed tuleb pseudonüümida või täita tuleb IKS-i lisanõudeid 25
2.4.2. Viidata tuleb õigusakti sättele 26
2.5. Kuidas tagada isikuandmete seaduslik töötlemine? 27
2.5.1. Õiguslik alus määratakse enne isikuandmete töötlemisega alustamist 27
2.5.2. Määrata tuleb kõige asjakohasem õiguslik alus 27
2.5.3. Eristada tuleb teadustööga kaasnevat tegevust, mis võib vajada omaette õiguslikku alust 28
2.5.4. Inimestele on antud võimalikult suur otsustamisvabadus 28
2.6. Kuidas tagada isikuandmete õiglane töötlemine? 28
2.6.1. Isikuandmete töötlemine on kooskõlas inimese ootustega 28
2.6.2. Vastutava töötlejaga peab saama vahetult suhelda 29
2.6.3. Välditud on diskrimineerimist isikuandmete töötlemisel 29
2.6.4. Välditud on inimeste vajaduste või haavatavuse ärakasutamist 29
2.6.5. Välditud on võimupositsiooni 30
2.6.6. Isikuandmete töötlemine on eetiline 30
2.7. Kuidas tagada isikuandmete läbipaistev töötlemine? 30
2.7.1. Antav teave on selge, arusaadav ja asjakohane 30
2.7.2. Teabe esitamiseaeg ja kanal on sobivad 30
2.7.3. Kasutatavate algoritmide kohta antakse teavet 31
2.7.4. Kaasvastutuse korral on selgelt eristatud, mille eest ja mil määral keegi vastutab 31
2.8. Mida pidada silmas teiseste isikuandmete kasutamisel? 31
2.8.1. Teisene kasutus võib olla kooskõlas esialgse eesmärgiga 32
2.8.2. Teabe andmine andmesubjektile teiseste andmete kogumisel 32
2.8.3. Teiseste andmete valdajad 32
2.8.4. Teiseseks kasutuseks tuleb leida sobiv õiguslik alus 33

2.8.5. Eriliiki isikuandmete jaoks on nõutav eetikakomitee kooskõlastus ... 33
2.8.6. Teiseste andmete edastamiseks võib olla vaja sõlmida leping ... 33
2.8.7. Avalikustatud isikuandmete teisene kasutamine ... 34
2.9. Kuidas arvestada teadustöös inimeste õigustega oma andmete üle? ... 34
2.9.1. Õigus saada teavet isikuandmete töötlemise kohta ... 34
2.9.2. Õigus andmetega tutvuda ... 35
2.9.3. Õigus andmete parandamisele ... 35
2.9.4. Õigus andmete kustutamisele ... 36
2.9.5. Õigus andmete töötlemise piiramisele ... 36
2.9.6. Andmete ülekandmise õigus ... 37
2.9.7. Õigus esitada vastuväiteid ... 37
2.9.8. Õigus olla kaitstud automatiseeritud töötlemisel põhinevate otsuste eest ... 37
2.10. Mida pidada silmas haavatavate isikute andmete töötlemisel? ... 38
2.10.1. Haavatavad isikud ja rühmad ... 38
2.10.2. Haavatava isiku nõusolek ei pruugi olla vabatahtlik ... 38
2.10.3. Haavatavate isikute andmete töötlemine võib ohustada nende õigusi ja huve ... 39
2.11. Mida pidada silmas eriliiki isikuandmete töötlemisel? ... 39
2.11.1. Eriliiki isikuandmete nõusolekuta töötlemiseks peab olema eetikakomitee kooskõlastus 39
2.11.2. Eriliiki isikuandmete töötlemine vajab lisakaitsemeetmeid ... 39
2.11.3. Eriliiki isikuandmete mõiste kohaldamine on kohati keeruline ... 39
2.12. Kui täpselt tuleks sõnastada teadusuuringu eesmärk? ... 39
2.13. Millal on tarvis eetikakomitee kooskõlastust? ... 40
2.13.1. Seadusest tulenev kohustus ... 40
2.13.2. Rahastajate ja kirjastajate nõuded ... 41
2.13.3. Eetilised kaalutlused ... 41
2.14. Kuidas hinnata isikuandmete töötlemisega kaasnevaid riske? ... 41
2.14.1. Riskihindamise üldmeetod ... 41
2.14.2. Isikuandmete töötlemisega seotud ohtude hindamine ... 43
2.14.3. Andmekaitsealase mõjuhinnangu koostamine ... 43
2.15. Mida pidada silmas laste isikuandmete töötlemisel? ... 45
2.15.1. Alaealine ei saa anda nõusolekut, kuid ta peab oma andmete töötlemisega nõustuma ... 45
2.15.2. Lapsele tuleb anda teavet tema andmete kasutamise kohta lihtsas ja selges keeles ... 45
2.15.3. Lapse isikuandmete töötlemise õiguslik alus ei saa olla õigustatud huvi ... 45

2.16. Mida pidada silmas surnud isikute andmete töötlemisel? 46
2.16.1. Surnud isikute andmete kaitse eesmärk on kaitsta teisi inimesi 46
2.16.2. Pärast surma läheb nõusoleku andmise ja tagasivõtmise õigus pärijatele 46
2.16.3. Muud andmesubjekti õigused pärijatele üle ei lähe 46
2.16.4. Teadlasel ei ole kohustust pidada arvet uuritavate elu ja surma üle 47
2.16.5. Surnute andmeid võib muul õiguslikul alusel töödelda 47
3. Teadustöö tegemine: andmete kogumine ja analüüs 48
3.1. Kuidas tagada, et isikuandmete töötlemine oleks turvaline? 48
3.1.1. Infoturbe süsteemne haldamine 48
3.1.2. Vajaduspõhine juurdepääs isikuandmetele 49
3.1.3. Andmete turvaline edastamine 49
3.1.4. Andmete turvaline talletamine 49
3.1.5. Andmete varundamine 50
3.1.6. Teadlikkus rikkumisvõimalusest 50
3.1.7. Isikuandmete töötlemiseks sobivad teenused, tarkvara ja vahendid 50
3.2. Mida pidada silmas, kui isikuandmeid edastatakse ühest riigist teise? 51
3.2.1. Euroopa Liidu liikmesriigid, Island, Liechtenstein ja Norra 51
3.2.2. Piisava andmekaitse tasemega kolmandad riigid 52
3.2.3. Muud kolmandad riigid 52
3.3. Miks ja kuidas isikuandmeid pseudonüümida? 52
3.3.1. Andmete pseudonüümimise põhjused ja aeg 53
3.3.2. Andmete pseudonüümijad 53
3.3.3. Andmete pseudonüümimise meetodid 53
3.4. Miks ja kuidas isikuandmeid anonüümida? 54
3.4.1. Andmete anonüümimise põhjused ja aeg 55
3.4.2. Andmete anonüümijad 55
3.4.3. Andmete anonüümimise meetodid 55
3.4.4. Andmete ja isikute seostamise vältimine 56
3.4.5. Kuidas teha anonüümset küsitlust? 57
3.5. Mida teha andmekaitsealase rikkumise korral? 58
3.5.1. Andmekaitsealasest rikkumisest tuleb kohe teada anda 58
3.5.2. Pärast rikkumisest teavitamist tuleb olla valmis teabe jagamiseks 59
3.5.3. Rikkumise võimalikud tagajärjed 59

3.6. Mida teha, kui andmesubjektilt tuleb päring oma andmete kohta? 59
4. Teadustöö tulemuste avaldamine ja andmete säilitamine 61
4.1. Kui kaua võib teadustöös kasutatud isikuandmeid säilitada? 61
4.2. Millisel kujul võib isikuandmeid avaldada? 62
4.2.1. Andmete avaldamine isikustatud kujul 63
4.2.2. Andmete avaldamine pseudonüümitud kujul 63
4.2.3. Andmete avaldamine anonüümitud kujul 63
4.3. Kellega võib teadustööd tehes isikuandmeid jagada? 63
4.3.1. Andmete töötlemine uurimisrühmas 64
4.3.2. Andmete töötlemine mitme teadusasutuse koostöös 64
4.3.3. Andmete töötlemine juhendaja ja juhendatava koostöös 64
4.3.4. Andmete jagamine teiste teadlaste, kirjastuste, repositooriumide või avalikkusega 64
4.3.5. Andmete jagamise tingimused kirjastustes 65

1. Andmekaitse põhimõisted

Selles peatükis on selgitatud peamisi isikuandmete kaitse põhimõisteid ja seda, kuidas need on seotud teadustööga. Samuti on esitatud lühiülevaade sellest, kuidas isikuandmete töötlemist õiguslikult reguleeritakse ning kuidas see on seotud teaduseetikaga.

1.1. Mis on isikuandmete kaitse?

Isikuandmete kaitse (edaspidi ka: andmekaitse) eesmärk on kaitsta inimest ja tema eraelu. Euroopa Liidu toimimise lepingus ja Euroopa Liidu põhiõiguste hartas sätestatakse õigus isikuandmete kaitsele iseseisva põhiõigusena, mis näitab ühemõtteliselt selle vajalikkust ja olulisust.

Andmekaitset mõistetakse siinses juhendis kui õigusvaldkonda, mis reguleerib isikuandmete kasutamist. Ühelt poolt hõlmab see põhimõtteid, mis võivad tunduda iseenesestmõistetavad: näiteks vabatahtlikkuse põhimõte, mille kohaselt ei või küsida inimeselt tema andmete töötlemise kohta nõusolekut ähvarduste või sunniga, või inimese autonoomia austamine, mis tähendab, et igaüks peaks saama oma isikuandmete kasutamist kontrollida. Teiselt poolt põrkub isikuandmete kaitse mitme teise olulise eesmärgi ja huviga, nagu avaliku korra tagamine, teadustöö tegemine või ettevõtlus. Vastandlike huvide lahendamiseks on loodud erandeid, eeskirju ja põhimõtteid, mis ei pruugi aga enam olla endastmõistetavad.

Selles juhendis selgitatakse erandeid, mis kehtivad isikuandmete töötlemisel teadusuuringutes. Sealjuures tuleb arvestada, et andmekaitsevaldkond on lai ning ühiskonna ja tehnoloogia arengu tõttu tekib pidevalt lahendamist vajavaid uusi küsimusi.

Andmekaitse Tartu Ülikoolis

Tartu Ülikooli siseveebist leiab lühijuhised mitmesugustel isikuandmete töötlemise teemadel. Lisaks antakse ülikoolisisesel vikilehel ülevaade peamistest andmekaitsepõhimõtetest valdkondade kaupa. Ülikooli töötajatele on koostatud andmekaitsemoodul, mida läbides saab ennast proovile panna ja oma teadmisi täiendada. Andmekaitse üldtingimustega on võimalik tutvuda ülikooli veebilehel ning asjaajamiseeskirja IX peatükis selgitatakse ülikooli töötajate õigusi ja kohustusi isikuandmete töötlemisel. Ülikooli avalikel vikilehtedel kirjeldatakse, kuidas tegutseda infoturbe- ja andmekaitseintsidentide korral.

1.2. Millised on peamised isikuandmete kaitse õigusaktid?

Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrusega (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (lühidalt: isikuandmete kaitse üldmäärus, IKÜM; siin edaspidi: üldmäärus) on kehtestatud üldised andmekaitsepõhimõtted igat laadi isikuandmete töötlemise, sh teadusuuringute suhtes. Üldmääruse jõustumisega toimus mitu olulist muutust andmekaitse õigusnormistikus.

Esiteks on üldmäärus **otsekohalduv**, st see kehtib vahetult sellises sõnastuses, nagu ta kirja on pandud. Erinevalt direktiividest ei pea üldmäärust Eestis seadusega üle võtma ega seda eraldi õigusaktiga kehtestama, kuid seda tuleb täita. Lisaks on Eestis muudetud ligikaudu 130 õigusakti, et viia need üldmäärusega kooskõlla.

Üldmäärusega on Euroopa Liidu liikmesriigid kokku leppinud üldised põhimõtted, kuid see ei paku üksiklahendusi ühe või teise olukorra jaoks. Seepärast on inimeste abistamiseks kirja pandud hulk suuniseid, soovitusi ja parimaid tavasid, mis aitavad üldmääruses sätestatut selgitada. Ka selle juhendi eesmärk on juhtida tähelepanu sellele, kuidas teadustöö tegemisel isikuandmete kaitsmise kohustusega arvestada.

Teiseks on igale Euroopa Liidu liikmesriigile jäetud võimalus **täpsustada seadusega** mõningaid olulisi **erandeid**. Isikuandmete töötlemine teadustöös on üks valdkondi, mida iga liikmesriik reguleerib oma seadusega. Eestis on selleks isikuandmete kaitse seadus (IKS), kus on näiteks täpsustatud eetikakomitee kooskõlastuse vajadust, mida üldmääruses ei käsitleta. Seega on isikuandmete töötlemisel teadustöös olukord tavapärasest keerulisem, kuna järgida ja tunda tuleb nii üldmäärust kui ka IKS-i.

Mis muutus üldmääruse jõustumisega?

Euroopa Liidu andmekaitsereformi käigus täpsustati mitut varem kehtinud põhimõtet ja kehtestati isikuandmete töötlejatele lisanõudeid. Allpool on nimetatud mõningad olulisemad muudatused, mis puudutavad teadustöö tegemist.

Muutusid terminid: senised *kodeerimine* ja *dekodeerimine* asendati *pseudonüümimisega*; termini *delikaatsed isikuandmed* asemel võeti üldmääruses kasutusele *isikuandmete eriliigid*, mis aga sõnastati IKS-is ümber *eriliiki isikuandmeteks*. Ka siinses juhendis kasutatakse Eesti õigusruumis levinumat terminit *eriliiki isikuandmeid*.

Kaotati vastutava töötleja registreerimise nõue: varem oli Eestis süsteem, kus eriliiki isikuandmete töötlejail tuli end Andmekaitse Inspektsioonis registreerida. Sellist registreerimissüsteemi enam ei ole. Eriliiki isikuandmete nõuetekohase töötlemise tagamiseks on kehtestatud üldine tingimus pidada nõu eetikakomiteega, sobiva komitee puudumisel Andmekaitse Inspektsiooniga.

Vastutava töötleja uued kohustused: Tartu Ülikoolile kui vastutavale töötlejale lisandus mitu kohustust: andmekaitsetingimuste avaldamine, isikuandmete töötlemise ülevaate koostamine, andmekaitsespetsialisti määramine, andmekaitsealaste mõjuhinnangute koostamine, järelevalveasutusega konsulteerimine ja rikkumistest teavitamine.

Avalike isikuandmete töötlemine on piiratud: varem oli IKS-i alusel kehtestatud erand, mille kohaselt oli õiguspäraselt avalikustatud isikuandmete edasine töötlemine alati lubatud.[1] Sellist erandit enam ei ole, mis tähendab, et ka avalikustatud isikuandmete töötlemiseks peab olema õiguslik alus, vastasel korral on töötlemine ebaseaduslik.

Kehtestati trahvid: Andmekaitse Inspektsiooni volitusi laiendati õigusega määrata andmekaitserikkumiste eest trahve, mis võivad Euroopa Liidus ulatuda ettevõtete puhul kuni 4%-ni üleilmsest aastasest kogukäibest ja muude isikute puhul 20 miljoni euroni.

[1] Kuni 01.01.2019 kehtinud seaduses § 11 lg 1. Samas hindas Riigikohus juba oma 2012. aasta otsuses 3-3-1-3-12, et IKS-i § 11 lg 1 ei andnud iseseisvat õiguslikku alust andmete töötlemiseks. Seega ei ole tegemist põhimõttelise muutusega, vaid pigem suurenenud selgusega.

1.3. Mis on isikuandmed?

Isikuandmed on mistahes andmed tuvastatud või tuvastatava isiku kohta. Isik on tuvastatav, kui ta on oma andmetega seostatav. Kui andmed ei ole seostatavad või neid on anonüümitud ehk töödeldud selliselt, et seostamine ei ole enam võimalik, siis ei ole tegemist isikuandmetega ja neile andmekaitse ei laiene. See, kas teadlane peab andmekaitse nõudeid järgima või mitte, sõltub niisiis tuvastatavuse võimalusest.

Isikut saab **tuvastada otseselt**, kui andmetes sisaldub näiteks nimi, isikukood või mõni muu kordumatu andmeüksus. Otsene tuvastamine piirdubki olemasolevate andmetega ja sel juhul ei ole tuvastamiseks lisaandmeid või -teadmisi vaja. **Kaudne tuvastamine** tähendab, et seos isiku ja tema andmete vahel ei avaldu otseselt, vaid see tuleb luua või tuletada näiteks mitme tunnuse kombineerimise abil. Kaudne tuvastamine võib olla võimalik ka eri andmestikke ühendades. Selline tuvastamine on hinnanguline.

Kui teadlane hakkab andmete tuvastatavust hindama, ei piisa seepärast vaid töödeldavatele andmetele otsa vaatamisest, vaid mõelda tuleb paar sammu kaugemale: mida on võimalik nende andmetega veel teha, kui on huvi nende taga olevad inimesed välja selgitada või üles leida. Kui isiku kohta on palju taustainfot, võib see muuta ka esmapilgul anonüümsena näivad andmed temaga seostatavaks.

Tuvastatavuse hindamisel tuleb arvesse võtta kõiki mõistlikke ja lihtsasti tehtavaid toiminguid, mille abil saab inimese tuvastada. Isikut ei peeta tuvastatavaks, kui see nõuab ebamõistlikult palju aega, vaeva või vahendeid. Mõistlikkuse hindamise aluseks on tuvastamisele kuluv ressurss võrrelduna tuvastamise tõenäosusega. Oluline on arvestada, et piir, kust alates ei ole enam isik tuvastatav, ei ole üheselt selge, ning seda hinnatakse aeg-ajalt uute tehnoloogiate ja identifitseerimismeetodite valguses ümber.

Üldistatult saab teadustööga seoses eristada kolme eri otstarbega isikuandmeid.

1. **Teadusandmed** on inimestelt või inimeste kohta kogutud andmed, mille töötlemine on vajalik uuringu eesmärkide saavutamiseks, näiteks intervjuude salvestised ja transkriptsioonid, küsitluste vastused, vaatlus- ja asukohaandmed, eksperimentide tulemused, terviseandmed, mõõtmistulemused või muud inimesega seostatavad andmed.
2. **Kontaktandmed ja muu töökorralduslik teave** on inimeste uuringus osalemisega seotud andmed, näiteks kutsutute nimekirjad, e-posti aadressid, telefoninumbrid, eksperimendi, intervjuu või muud tüüpi andmekogumise koha ja ajaga seotud andmed ning kirjalikud nõusolekuvormid. Need andmed kogunevad teadusuuringute käigus, kuid neid ei kasutata otseselt uuringus teaduslike eesmärkide saavutamiseks. Sellegipoolest on tegemist isikuandmetega, mille töötlemine peab vastama andmekaitsepõhimõtetele.
3. **Teadlaste kohta käivad andmed:** uuringu käigus võib koguneda hulk andmeid ka teadlaste kohta, näiteks teadustöö tegijate üld- ja kontaktandmed, töökoormuse, töötasu ja lähetuste andmed või teave selle kohta, kes, millal ja kuidas andmeid kogus ja analüüsis. Isikuandmed on ka teadusprojektide taotlustes esitatavad elulood. Paljud teadlaste andmed on avaldatud näiteks ETIS-es või teadusasutuse veebilehel.

Ülikooli andmekaitse vikilehelt leiab kontrollnimekirja, mis sisaldab teadusuuringu andmetöötluse kõiki etappe. Nende põhjal saab enne uuringu alustamist hinnata, kas kõik isikuandmete turvalise ja asjakohase töötlemise tingimused on täidetud.

Isikut, kelle andmeid töödeldakse, nimetatakse **andmesubjektiks**.

1.3.1. Eriliiki isikuandmed

Tavaliste isikuandmete kõrval eristatakse üldmääruses **eriliiki isikuandmeid**, mis on artikli 9 kohaselt

- andmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine,
- geneetilised andmed,
- füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed,
- terviseandmed või
- andmed füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta.

Üldjuhul on eriliiki isikuandmete töötlemine keelatud, st kehtib **töötlemispiirang**. Selliseid andmeid on lubatud töödelda vaid isiku nõusolekul või muude üldmääruse artikli 9 lg-s 2 sätestatud erandite korral. Samuti peab töötlemiseks olema õiguslik alus.

Näiteid eriliiki isikuandmete kasutamisest teadustöös

Hariduslik erivajadus. Kui teadlane soovib uurida õpilaste hariduslikke erivajadusi, võib tal olla keeruline hinnata, kas need on alati eriliiki isikuandmed. Kindlasti on see nii juhul, kui hariduslik erivajadus tuleneb tervislikest põhjustest (näiteks on seotud meditsiinilise diagnoosi või puudega). Kui aga erivajaduseks on andekus või suhtlemis- ja õpiraskused, ei pruugi see olla seotud lapse tervisega ja sel juhul ei ole tegemist eriliiki isikuandmetega. Sellegipoolest võib hariduslikku erivajadust pidada tavapärasest tundlikumaks andmeliigiks, eriti laste puhul.

Lõpphinnang sõltub konkreetsest andmetöötlusest ja selle eesmärgist. Kui eesmärk on teha vaid üldistusi ja uurijaid ei huvita erivajaduse põhjus, ei ole tegemist eriliiki isikuandmetega. Näiteks kui väidetakse, et ühes klassis on õpilastel A ja B mingi hariduslik erivajadus (täpsustamata konkreetselt), kuid õpilastel C, D ja E mitte, siis vaadeldakse erivajaduse fakti kui sellist, mis ei ole eriliigina käsitletav. Kui aga uuritakse teatud õpilaste toimetulekut kindla ja selgelt sõnastatud erivajaduse tõttu (näiteks kuidas kõnepuue mõjutab õpimotivatsiooni või millist tuge vajavad füüsilise puudega õpilased), siis on tegu eriliiki isikuandmete töötlemisega.

Kui teadlane ei saa andmekogumisel andmete hulka täielikult kontrollida (näiteks ei saa ta teada, kuidas intervjueeritav vastab või mida kirjutatakse avatud küsimuse vastuseks), võib tema kätte sattuda eriliiki isikuandmeid isegi juhul, kui algne eesmärk oli uurida eriliikide alla mittekuuluvaid erivajadusi (näiteks andekust). Seepärast on soovitatav käsitleda kõiki hariduslikke erivajadusi ettevaatuse mõttes eriliiki isikuandmetena, eriti kui ei saa välistada, et teadustöös analüüsitakse ka erivajaduste põhjuseid. Kui on teada, et seda ei tehta, tuleks see selgelt esile tuua uuringu kavas ja uuritavale antavas teabes. Samuti võib sõnastada andmekogumisel küsimused nii, et see ei innustaks kedagi terviseandmeid jagama.

Terviseindeksid. Indeksid ja muud kompleksed mõõdikud, mille põhjal saab teha järeldusi inimese tervise kohta, on käsitletavad terviseandmetena ja neid tuleb seetõttu pidada eriliiki isikuandmeteks. Sama kehtib ka indeksite arvutamise kohta. Kui teadustöö eesmärk on näiteks arvutada kehamassiindeksit, seostada see inimesega ja saada sel viisil uut teavet tema tervise kohta, tuleb indeksi arvutamist pidada eriliiki isikuandmete töötlemiseks. Samas ei ole kehakaal ja pikkus iseenesest eriliiki isikuandmed.

1.3.2. IP-aadressid

Euroopa Kohus on 19. oktoobri 2016. aasta otsuses C-582/14 hinnanud, et dünaamilised IP-aadressid, mis iga internetiühenduse puhul muutuvad, on isikuandmed. Selline tõlgendus põhineb üldmääruse

definitsioonil: isikuandmed on „igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada“.

Euroopa Kohus nendib, et „dünaamiline IP-aadress ei kujuta endast teavet, mis puudutab „tuvastatud füüsilist isikut“, kuna selle aadressi põhjal ei selgu otse selle füüsilise isiku identiteet, kellele kuulub arvuti, millest külastati veebilehte, ega ka ühegi teise isiku oma, kes seda arvutit võis kasutada“ (p 38). Siiski on IP-aadressi kaudu võimalik isikut **kaudselt** tuvastada. Euroopa Kohus on selgitanud, et kõik tuvastamiseks vajalikud andmed ei pea olema ühe isiku valduses (p 43). See tähendab, et internetiteenuse pakkujalt võib küsida andmeid juurde, misjärel muutub isiku tuvastamine ikkagi võimalikuks.

Lisaks tuleks hinnata, kuivõrd **mõistlik ja tõenäoline** on võimalus, et eri andmete ühendamisel isik kaudselt tuvastatakse. Kohtu hinnangul on näiteks mõistlik ja tõenäoline see, kui isikute õiguste kaitseks või seaduslike kohustuste täitmiseks edastab internetiteenuse pakkuja oma kliendi andmed pädevale asutusele (näiteks küberrünnakute puhul). Sealjuures on ka potentsiaalse õigusrikkuja dünaamilise IP-aadressi teadjal võimalik pöörduda enda õiguste kaitseks või oma seaduslike kohustuste järgimiseks kohtu või muu pädeva asutuse poole, kes saab nõuda internetiteenuse pakkujalt vajalikke andmeid IP-aadressi taha peituva õigusrikkuja tuvastamiseks.

Mõistlik ja *tõenäoline* hõlmavad järelikult võimalust, et isik tuvastatakse kaudselt mitme asutuse või isiku koostöös. Ebamõistlik ja ebatõenäoline on kaudne tuvastamine, mis on seadusega keelatud, praktiliselt teostamatu või eeldab ülemäärast pingutust või kulutust (p 46). Järelikult tuleb teadlasel arvestada, et kui näiteks veebiküsitluse või muu veebipõhise teenuse vahendusel kogutud andmetega koos salvestub ka vastaja IP-aadress, võib see muuta vastaja andmekaitse õiguse vaatepunktist tuvastatavaks. Mitmesugused küsitluskeskkonnad võimaldavad teadlasel seadistada küsitlus selliselt, et vastaja kohta ei kogutaks IP-aadressi ega muid tehnilisi andmeid, mis lihtsustaksid tema tuvastamist (vt p 3.4.5).

1.4. Mis on isikuandmete töötlemine?

Töötlemine on andmekaitsealane üldtermin andmetega tehtavate kõikvõimalike toimingute kohta. Selle alla kuuluvad andmete kogumine, salvestamine, kopeerimine, muutmine, süstematiseerimine, pärimine, edastamine ja hävitamine. Isikuandmete töötlemine kestab andmete saamisest kuni nende hävitamiseni ja hõlmab kõiki toiminguid, mis jäävad nende vahele.

Töötlemiseks loetakse ka isikustatud või pseudonüümitud andmete anonüümimist, mis peab koos sellele eelneva andmete kogumisega vastama üldistele andmekaitsepõhimõtetele.

Üldmääruses eristatakse isikuandmete töötlemisel kolme vastutavat rolli.

1. **Vastutav töötleja** on isik või asutus, kes määrab töötlemise eesmärgid ja vahendid ehk kontrollib sisuliselt isikuandmete töötlemist. Vastutav töötleja on enamasti juriidiline isik, kelle juures isikuandmete töötlemine toimub. Tartu Ülikool on vastutav töötleja asutusena, teadlane aga vastutab kõige selle eest, mida ta oma töös isikuandmetega teeb. Tema seab andmetöötluseesmärgid ja ütleb, milliseid andmeid ta kogub ja milliste vahenditega.

See, et ülikool võib olla isikuandmete vastutav töötleja, ei tähenda, et iga ülikooli töötaja pääseb isikuandmetele juurde. Juurdepääs peab olema vajaduspõhine ja piiritletud teadlastega, kes on konkreetse projekti või uuringuetapiga seotud. Kui tegu on tundlike andmetega, näiteks laste või eriliiki isikuandmetega, tuleb ligipääsu veelgi kitsendada neile teadlastele, kel on tingimata vaja isikustatud andmeid töödelda.

2. Kui isikuandmete kohta teevad otsuseid mitu asutust ühiselt, näiteks ülikool koos teiste teadusasutustega, on nad **kaasvastutavad töötlejad**. Kaasvastutus eeldab, et koostööasutused määravad töötlemise eesmärgid ja vahendid ühiselt. Näiteks Euroopa Liidu rahastatud projektide puhul on võimalik, et projekti partnerid vastutavad kas igaüks enda tegevuse eest või on kaasvastutajad sõltuvalt töö- ja otsustuste jaotusest.

3. **Volitatud töötleja** on isik või asutus, keda vastutav töötleja on eraldi lepingu alusel volitanud isikuandmeid töötlema. Volitatud töötleja tegutseb vastutava töötleja nimel, kuid kuna ta ei saa määrata ega muuta isikuandmete töötlemise eesmärke ja vahendeid, ei ole ta vastutav töötleja. Ülikoolis töölepinguga töötav inimene ei ole volitatud töötleja, sest ülikool ei saa iseennast volitada. Kuid selleks võib olla näiteks ülikooli teadlane, keda mõni muu avalik või eraasutus on eraldi kokkuleppe alusel palganud analüüse või ekspertiisi tegema.

Enamasti ei ole teadlane siiski ei volitatud ega vastutav töötleja: ta täidab oma tööülesannete kaudu ülikooli kui vastutava töötleja kohustusi. Kui teadlane on näiteks rahvusvahelise teadusprojekti põhi- või vastutav täitja, on kogu projekti vältel vastutav või kaasvastutav töötleja – olenevalt teadusasutuste kokkuleppest – tema ülikool. See ei tähenda mõistagi, nagu oleks teadlane vastutusest vabastatud. Hea tava on määrata konkreetses uuringus töödeldavate andmete eest eraldi **vastutav uurija**, kes peab tagama andmetöötluse korrektsuse. Tema ülesanne on kindlustada andmete konfidentsiaalne ja turvaline töötlemine ning juhendada isikuandmeid töötlevaid teadlasi.

Nii vastutav uurija kui ka vastutav töötleja peavad järgima andmekaitsepõhimõtteid, kuid erinev on see, kellele nad aru annavad. Vastutav töötleja ehk ülikool annab andmekaitsealase rikkumise korral aru Andmekaitse Inspektsioonile, vastutav uurija enda tööandjale ehk ülikoolile, samuti tuleb tal teavitada ülikooli andmekaitse peaspetsialisti. Ülikooli kohustus on hinnata isikuandmete töötlemisega seotud võimalikke riske ja võtta meetmeid nende maandamiseks, kuid riskianalüüsi koostamine on teadlase tööülesanne.

Niisiis sõltub teadlaste ja ülikooli kokkuleppest, millised andmekaitsekohustused on millise töötaja kanda. Ülikooli asjaajamiseeskirjas on sätestatud, et isikuandmete kaitse eest vastutavad andmekaitse spetsialist, struktuuriüksuse juht ja isikuandmeid töötlev töötaja. Igal isikuandmeid töötleval töötajal kohustus tagada andmete terviklus ja konfidentsiaalsus. Struktuuriüksuse juhil tuleb tagada kõikide isikuandmete töötlemise toimingute registreerimine.

Kolmas isik on isik või asutus, kes ei ole ei andmesubjekt, vastutav ega volitatud töötleja ega tööta vastutava ega volitatud töötleja alluvuses. Lihtsustatult on see isik, kel ei ole isikuandmete töötlemises selget rolli. Teadustöö puhul võivad kolmandad isikul olla näiteks teadlase pereliikmed, töö oponent või retsensent, tööd publitseeriva kirjastuse töötajad jne.

Lisaks eristatakse andmekaitses **vastuvõtjaid** ehk isikuid või asutusi, kellele andmeid õiguslikul alusel edastatakse, kuid see on vaid olukorrapõhine roll. Vastuvõtja võib olla nii vastutav töötleja, volitatud töötleja kui ka kolmas isik.

Iga asutus, sh ülikool kehtestab **andmekaitsetingimused**, mida peab järgima iga teadustöösse kaasatud isik alates intervjuud transkribeerivast üliõpilasest kuni teadusprojekti juhtiva professorini. Tingimusi tuleb täita ka vaatamata töötlemise eesmärgile. Ülikoolis kehtivad samad tingimused nii personali-, õppe- kui ka teadustööga seotud isikuandmetele. Teadustöö eesmärk ei vähenda vajadust isikuandmeid kaitsta või isikute õigustega arvestada.

1.5. Millised on andmekaitsepõhimõtted?

Kogu andmekaitse õiguslikul reguleerimisel lähtutakse üldmääruse artiklis 5 sätestatud isikuandmete töötlemise põhimõtetest (edaspidi: andmekaitsepõhimõtted). Need kehtisid ka enne üldmääruse vastuvõtmist, kuid nende tõlgendamine ja rakendamine on aja jooksul veidi muutunud.

1.5.1. Isikuandmete töötlemine on seaduslik ja õiglane

Isikuandmete töötlemine on seaduslik, kui sellel on õiguslik alus. Selle puudumisel on isikuandmete töötlemine ebaseaduslik.

Õiglane tähendab, et andmesubjekti huve ja õigusi tuleb arvesse võtta ning neid ei tohi ülemäära kahjustada. Isegi kui töötlemine on seaduslik, võib see ebaproportsionaalselt inimest kahjustada ja olla seega ebaõiglane.

1.5.2. Isikuandmete töötlemine on läbipaistev

Läbipaistvus tähendab, et andmesubjekt mõistab, mida ja kuidas tema andmetega tehakse, ning et sellekohane info on arusaadav ja lihtsasti leitav. Läbipaistvuspõhimõttest tulenevad näiteks teavitamise ja andmekaitsetingimuste avaldamise kohustus.

1.5.3. Isikuandmete töötlemine on eesmärgipärane

Eesmärgipärasuse põhimõte tähendab üldiselt, et enne andmete kogumist peab nende töötlemise eesmärk olema õiguspärane ning selgelt ja täpselt sõnastatud. Näiteks ei ole korrektne nimetada eesmärgiks „teadustöö“ või „teadusuuring“, vaid konkreetne projekti või uuringu lõpptulemus. Samas on üldmääruse põhjenduses 33 nõusoleku küsimise kohta nenditud, et alati ei ole võimalik teadusuuringus tehtava andmetöötluse eesmärki täielikult kindlaks määrata, mistõttu on lubatud nimetada see teadusuuringu valdkonna või teadusprojekti osa täpsusega.

Kui üldjuhul ei tohi muudel kui eelnevalt kindlaks määratud eesmärkidel andmeid töödelda, siis teadustöö kohta on üldmääruses tehtud sellele põhimõttele erand: algul teistel eesmärkidel kogutud andmeid on lubatud kasutada hilisemas teadustöös. IKS-i § 6 lg-s 1 sätestatakse sealjuures kohustus andmed enne teadusuuringuks üleandmist pseudonüümida.

Arvestama peab ka sellega, et akadeemilise töö eesmärk katab vaid otseselt uuringuga seotud toimingud, kuid peale teadusliku uurimise kaasneb tööga ka muu tegevus. Kui isikuandmeid kasutatakse näiteks publikatsioonides, õppetöös, teaduskonverentsidel, ettevõtluses, teadustulemuste rakendamisel või teaduse populariseerimisel, vajavad need omaette eesmärgi ja õigusliku aluse kindlaksmääramist.

Eesmärgipärasust on keeruline hinnata, kui ei tea, milliseid andmeid kogutakse. Seepärast on hea tava määrata eesmärk konkreetsete andmesubjektide või andmetüüpide kaupa. Näiteks on ülikooli andmekaitsetingimustes kirjeldatud andmete kaupa nende töötlemise eesmärke ja õiguslikke aluseid.

1.5.4. Isikuandmete töötlemine on minimaalne

Minimaalsuspõhimõtte kohaselt tuleks koguda ja töödelda võimalikult vähe andmeid – üksnes neid, mis on teadustöö eesmärgi saavutamiseks vajalikud. Liigne andmete kogumine võib olla ebaseaduslik, kui selleks puudub eesmärgist tulenev selge vajadus. Seepärast tuleb minimaalsuspõhimõtte järgimiseks hoolikalt läbi mõelda, milliseid miinimumandmeid on eesmärgi täitmiseks vaja.

Näide

Sünnikuupäev annab inimese kohta rohkem teavet kui sünniaasta, sünniaasta rohkem kui vanus aastates, täpne vanus rohkem kui vanusevahemik. Kui teadusuuringus analüüsis soovitakse jaotada vastanud vanusevahemike järgi kohortidesse, siis on minimaalsuspõhimõttega vastuolus küsida inimese sünnikuupäeva või täpset vanust. Minimaalne lahendus oleks küsida kohe vastajalt, millisesse kohorti ta kuulub.

1.5.5. Isikuandmete töötlemine põhineb kvaliteetsetel andmetel

Õigsuspõhimõte tähendab, et töödelda võib vaid õigeid andmeid. Neid tuleb seepärast kontrollida, parandada ja vajaduse korral tuleb need ajakohastada või kustutada. Andmesubjektil on õigus nõuda ebaõigete andmete parandamist (vt p 2.9.3). Seda õigust võib ta alati rakendada ja selle suhtes ei ole ka teadustöö jaoks erandit tehtud.

Ent ka inimese ebaõiged andmed on käsitletavad isikuandmetena. Seega tuleb rakendada andmekaitse põhimõtteid ühtviisi kõigi andmete suhtes, sõltumata nende tõesusest.

Näide

Kui longituuduuringusse kaasatute kontaktandmed muutuvad, tuleks need avalikest andmekogudest saadud päringuvastuste põhjal parandada. Kuigi selline kontaktandmete päring on teadusuuringu vajadust arvestades põhjendatud, võib siiski küsimusi tekitada selle õiguslik alus – kas teadlastel on õigus andmekogust kontaktandmeid saada ja kas andmekogu vastutaval töötlejal on õigus neid teadlasele anda? Seega tekitab andmekvaliteedi nõude tagamine mõningast vastuolu.

Selguse huvides oleks kasulik küsida uuringus osalejatelt eraldi nõusolekut hilisemaks ühendusevõtmiseks või kontaktandmete uuendamiseks avalike andmekogude alusel.

1.5.6. Isikuandmete säilitamise piirang

Üldjuhul võib andmeid säilitada vaid seni, kuni eesmärk on täidetud, ja seejärel tuleb need kustutada või anonüümida. Pärast algse eesmärgi täitmist võib andmeid säilitada vaid juhul, kui töötlemine toimub avalikes huvides arhiveerimise, ajaloo- või teadusuuringu või statistilisel eesmärgil (vt ka alaptk 4.1).

1.5.7. Isikuandmete töötlemine on turvaline

Turvalisus tähendab, et tagada tuleb ühtaegu nii andmete käideldavus, terviklus kui ka konfidentsiaalsus ehk kaitstus volitamata töötlemise eest. Turvalisuse tagamiseks tuleb kasutusele võtta erinevaid tehnilisi ja korralduslikke meetmeid. Tehniliste meetmete hulka kuulub näiteks andmete krüpteerimine, korralduslikud meetmed hõlmavad näiteks juurdepääsuõiguste määramist teadlastele või andmete hoidmist ühes serveris, mitte iga teadlase isiklikus tööarvutis.

1.5.8. Lõimitud andmekaitse

Lõimitud andmekaitse eeldab vastutavalt ja volitatult töötlejalt kõigi andmekaitsepõhimõtete ja tööprotsesside lõimimist. See tähendab, et teadlane peab pöörama andmekaitseküsimustele jooksvalt ja läbivalt tähelepanu kõigis andmetöötlusetappides, alustades uurimistöö plaanimisest.

Lõimitud andmekaitse haakub privaatsuslõime (*privacy by design*) kontseptsiooniga, mis on välja kasvanud info- ja kommunikatsioonitehnoloogia arendamise põhimõtetest ning rõhutab eraelu ja isikuandmete läbiva kaitsmise olulisust. Sellest omakorda on kujunenud lõimitud väärtuste põhine lähenemisviis (*values by design; ethics by desgin*), mille puhul peetakse oluliseks, et tegevuse ja tööprotsesside kavandamisel lähtutaks inimlikest väärtustest.

Näide

Lõimitud andmekaitse põhimõtte rakendamisel küsitakse inimeselt ühe põhjaliku nõusoleku asemel eraldi nõusolekud nii uuringus kasutatavate isikuandmete töötlemiseks, juhuleidudest teavitamiseks, eri andmestike ühendamiseks, jätku-uuringus osalemiseks, isikuandmete kasutamiseks edasistes uuringutes kui ka isikuandmete säilitamiseks pärast plaanitava teadustöö lõppu. Kui nõusolekut küsitakse siiski mitme valiku kohta korraga, tuleb anda inimesele võimalus keelduda mõne eesmärgiga nõustumast.

1.5.9. Vaikimisi andmekaitse

Vaikimisi andmekaitse eeldab teadlaselt, et valikuvõimaluse olemasolul tuleb eelistada alati inimese eraelule suuremat kaitset pakkuvaid lahendusi. Kui näiteks intervjuudel põhineva uuringu tulemuste avaldamisel on võimalik valida, kas intervjueeritavate nimed avalikustada või jätta saladusse, tuleb vaikimisi eelistada nende konfidentsiaalseks jätmist. Kui andmete analüüsimise etapis oleks võimalik samad eesmärgid täita ka pseudonüümitud andmetega, tuleks otsustada viimase variandi kasuks.

Vaikimisi andmekaitse põhimõte on kesksel kohal ka inimeselt isikuandmete töötlemiseks nõusoleku küsimisel, mille puhul on vaikimisi vastus „ei“ ja osaleja peab aktiivselt oma nõustumist kinnitama (vt ka alaptk 2.3).

1.5.10. Pseudonüümimine ja anonüümimine

Üldmääruse kohaselt on **pseudonüümimine**[2] isikuandmete töötlemine selliselt, et isiku tuvastamist võimaldavad andmed on eemaldatud ja asendatud pseudonüümiga, näiteks koodi või muu tunnusega. Sellised andmed on aga endiselt isikuandmed, sest need saab tagasi pöörata isikustatud andmeteks. Pseudonüümimine on lisakaitsemeede, millega kaitstakse andmesubjekti õigusi, kuid ei vabasta teadlast vastutusest andmekaitsepõhimõtete järgimise eest (vt ka alaptk 3.3).

Anonüümimine on isikuandmete töötlemine selliselt, et inimese otsene ega kaudne tuvastamine ei ole ühelgi mõistlikul ja tõenäolisel viisil enam võimalik. Anonüümimisel ja pseudonüümimisel võivad olla sarnased andmetöötlusmeetodid, kuid nende peamine erisus on töötlemise *pöördumatus*: pseudonüümimine on tagasipööratav, anonüümimine mitte (vt ka alaptk 3.3).

Andmeid, mis käivad küll inimeste kohta, kuid ei ole seostatavad konkreetsete isikutega, nimetatakse **anonüümseteks andmeteks**, mille kasutamist andmekaitse ei reguleeri. Teadlasel tuleb hinnata, kas anonüümseid andmeid on mingil viisil võimalik siiski isikuga seostada või kui tõenäoline on see tulevikus.

[2] Üldmääruses on kasutatud terminit *pseudonümiseerimine.*

1.6. Mis on õiguslik alus?

Isikuandmete töötlemine on seaduslik vaid juhul, kui selleks esineb üks üldmääruse artiklis 6 nimetatud õiguslik alus. Need alused on koos lühikese selgitusega loetletud ka Andmekaitse Inspektsiooni koostatud isikuandmete töötleja üldjuhendis (lk 7–8).

Olenevalt uuringust tuleb teadlasel valida, millist õiguslikku alust kasutada.

Nõusolek on teadustöös kõige tavapärasem õiguslik alus. See toetab uuringusse kaasatud inimeste autonoomiat ja tagab, et nende osalemine on vabatahtlik. Nõusolek peab olema teadlik, mistõttu on nõusoleku küsimisele seatud mitmesuguseid lisanõudeid (vt alaptk 2.3).

Avalikes huvides olev ülesanne on õiguslik alus avalik-õiguslike teadusasutuste jaoks, kelle jaoks on see ülesanne õigusaktiga sätestatud. Näiteks on Rahvusarhiivile antud arhiiviseadusega ülesanne teha arhiivinduslikke teadusuuringuid ja neid publitseerida. Järelikult sobib Rahvusarhiivis tehtavate, isikuandmeid sisaldavate teadusuuringute õiguslikuks aluseks avalikes huvides olev ülesanne.

Avalikes huvides olev ülesanne ei sobi õigusliku alusena aga eraõiguslikele teadusasutustele, kelle uurimistegevuse jaoks eraldi õigusakte ei kehtestata. Samas võib eraõiguslik teadusasutus täita riigiasutuse tellimust või olla muul viisil volitatud tegema uuringut, mille õiguslik alus on avalikes huvides ülesanne.

Õigustatud huvi on paindlik alus, mis võimaldab vajaduspõhiselt hinnata, kuivõrd olulised on erinevad vastandlikud huvid. Vastutav töötleja peab kaaluma oma õigustatud huvi ja võimalike andmesubjektide huve. Seega ei piisa pelgalt sellest, et teadusasutusel esineb teadustöö suhtes õigustatud huvi või et see on avalikes huvides, vaid need huvid peavad olema kaalukad ning andmesubjektide huvide ja õiguste võimalik riive peab olema võimalikult väike.

Avalikud asutused saavad õigustatud huvi õigusliku alusena kasutada väga piiratud tingimustel (nt töötõendid, fotod siseveebis, kaamerate kasutamine). Seda saaksid aga teha eraõiguslikud teadusasutused või teadus- ja arendustööd tegevad ettevõtted.

Lisaks on üldmääruses veel kolm õiguslikku alust – seadusest tuleneva kohustuse täitmine, andmesubjektiga sõlmitud lepingu täitmine ja isiku eluliste huvide kaitsmine –, kuid need ei ole teadusuuringute kontekstis sobivad. Erandkorras võivad need alused osutuda siiski vajalikuks. Näiteks on lastekaitseseaduse § 27 kohaselt igaühel kohustus anda teada abivajajast lapsest. Seega, kui teadlane suhtleb uuringu eesmärgil laste või peredega, kelle suhtes tal tekib põhjendatud kahtlus, et laps vajab abi (näiteks on ta perevägivalla ohver), on teadlasel kohustus sellest kohalikku omavalitsust teavitada. Sellisel juhul on lapse isikuandmete avaldamise õiguslikuks aluseks seadusest tulenev kohustus. Isegi kui mõnikord väga harva võib teadustöö tegemisel selline vajadus tekkida, ei ole sel juhul siiski tegemist teadustöö eesmärgil isikuandmete töötlemisega.

1.7. Kuidas on hea teadustava seotud isikuandmete töötlemisega?

Euroopa Andmekaitseinspektor on oma esialgses arvamuses (lk 12) väljendanud seisukohta, et andmekaitse erandid kehtivad vaid eetiliselt tehtud teadustöö korral. Seega tuleb isikuandmete töötlemisel silmas pidada nii teaduseetika kui ka andmekaitse põhimõtteid.

Euroopas võeti 2017. aastal vastu Euroopa teaduseetikakoodeks, mis on „abistav teejuht teadlastele nende töös, samuti juhtudel, kui neil tuleb kokku puutuda teadustöös peituvate praktiliste, eetiliste ja intellektuaalsete probleemidega“. Koodeksis on kirjeldatud teaduseetika aluspõhimõtteid ja rikkumise viise.

Eestis on üldised teaduseetika põhimõtted kokku lepitud heas teadustavas, kus käsitletakse samu küsimusi mis siinses juhendis. Eetiliste ja õiguslike kohustuste vallas on palju kattuvat, kuid mõnes üksikküsimuses võivad eetilised kohustused nõuda teadlaselt rohkem, teisel juhul võib aga kehtida enam erandeid. Järgmistes peatükkides on kirjeldatud head teadustava, mis on seotud otseselt isikuandmete töötlemisega, eeskätt nõusoleku andmise, teavitamise, juurdepääsu ja andmete säilitamisega.

2. Teadustöö planeerimine

Selles peatükis on selgitatud peamisi isikuandmete töötlemisega seotud küsimusi, millele tuleks mõelda juba teadustööd planeerides. Oluliste teemadena on käsitletud isikuandmete töötlemise seaduslikkust ning nõusoleku alusel ja nõusolekuta tehtud uuringuid. Lisaks on selgitatud eriliiki isikuandmete töötlemise nõudeid ja andmesubjektide õigusi oma andmete suhtes.

Andmekaitsega tuleb tegeleda kogu teadustöö vältel ja pärast selle valmimistki. Ühelt poolt peab sellele **lõimitud andmekaitse** põhimõtte kohaselt mõtlema juba projektitaotluse koostamisel, kui täpsed ülesanded ja tööjaotus pole veel paigas. Teisalt võivad andmekaitsega seotud teemad esile kerkida aastaid pärast projekti lõppu, kui näiteks algsel eesmärgil kogutud andmeid soovitakse kasutada ka hiljem järgmises uuringus. Kui on juba ette teada, et andmestik on väärtuslik või see võib olla alus ka mõnele teisele teadustööle, tuleks küsida andmesubjektidelt sellekohane nõusolek juba enne algse töö andmete kogumist.

Kuna andmekaitseteemad kattuvad osaliselt **andmehalduse** teemadega, on soovitatav tegeleda mõlemaga korraga. Näiteks kui projekti raames on kavas isikuandmeid turvalisuse põhimõtte kohaselt pseudonüümida, saab juba varakult planeerida, kuidas seda teha, kellel on ligipääs võtmele või andmetele ning mida tehakse võtmega projekti lõpus. Kõik need otsused tasub kirjutada andmehaldusplaani (vt p 2.2.1).

2.1. Millega alustada, kui teadustöös on kavas isikuandmeid töödelda?

Kõigepealt tuleb koostada ülevaade plaanitavast teadustööst ja töödeldavatest isikuandmetest. Välja tuleb selgitada teadustöö jaoks kogutavate isikuandmetega seonduvad nõuded, kitsendused ja riskid, mis vajavad tähelepanu. Mida varem isikuandmetega seotud probleemid tuvastatakse, seda rohkem on aega nendega tegeleda.

Allpool on esitatud kontrollküsimustik, milles olevatele küsimustele on soovitatav teadustööd kavandades mõelda. Enne vastama hakkamist tasub tutvuda ka rahastaja tingimuste ja nõuetega, kuna sageli võivad need siinsete küsimustega kattuda, ehkki teistsuguses sõnastuses, järjekorras või detailsuses. Abiks on Euroopa Komisjoni teadustöö planeerimiseks loodud eetika ja andmekaitse otsustuspuu.

Vastused tasub kohe dokumenteerida. Kui teadustöö või -projekti jaoks on plaanis koostada andmehaldusplaan (vt p 2.2.1), on kõige mõistlikum küsimuste vastused sinna kirjutada. Lisaks võivad kirjalikud vastused olla abiks andmekaitsetingimuste, nõusolekuvormi, eetikakomitee kooskõlastuse taotluse, rahastustaotluse või muu isikuandmetega seotud dokumentatsiooni koostamisel.

KONTROLLKÜSIMUSTIK ISIKUANDMETE KASUTAMISE KOHTA TEADUSTÖÖS

1. Mis on teadustöö eesmärk?

Eesmärk tuleb sõnastada nii täpselt ja konkreetselt kui võimalik. Kõige üldisemalt peab eesmärk andma teadustööga tutvujale teavet selle kohta, mida uuritakse või soovitakse uuringu abil saavutada (vt alaptk 2.12).

2. Kas mul on vaja isikuandmeid töödelda?

Kui teadustöö eesmärgid on täidetavad ka isikuandmeteta, tuleb eelistada seda võimalust. See on hea mitmel põhjusel: vähendab isikuandmete kogumise ja korrektse haldamisega seotud ressursikulu, säästab uuringusse kaasatuid, vähendab isikuandmete väärkasutamisest või ebaturvalisest haldamisest tulenevaid riske ja väldib omakorda nendest riskidest tekkivat kahju inimeste eraelule. Võrdsete tingimuste korral tuleks valida vähemate isikuandmete töötlemist eeldav lahendus – see on kooskõlas minimaalsuspõhimõttega (vt p 1.5.4).

3. Milliseid isikuandmeid ma töötlen?

Koguda tuleb vaid neid andmeid, mis on eesmärgi täitmiseks vajalikud, st neid ei tohi koguda igaks juhuks. Teadustööks vajalikud isikuandmed tuleb dokumenteerida koos nende kasutamise eesmärgiga – see aitab luua parema ülevaate ja seeläbi paremini hinnata, kas kõiki andmeid on tingimata vaja.

Uuringus kasutatavad isikuandmed tuleks esitada liikide või kategooriate kaupa. Seda teavet saab kasutada andmehaldusplaani koostamisel ja teadusprojektide isikuandmete töötlemise ülevaates.

4. Kas ma töötlen eriliiki isikuandmeid?

Planeerimisetapis tuleb välja selgitada, kas kogutavate andmete seas on eriliiki isikuandmeid (vt p 1.3.1). Kui plaanis on eriliike töödelda, tuleb selleks küsida kooskõlastust valdkonna eetikakomiteelt (vt p-d 2.2.4 ja 2.8.5 ning alaptk 2.11).

5. Kes on teadustöö andmesubjektid?

Ülevaade andmesubjektidest tuleks esitada liikide või kategooriate kaupa. Kuna üldine inimeste jaotamise klassifikatsioon puudub, võib eelistada samu termineid, mida on kasutatud valimi koostamisel, näiteks „50–60-aastased“, „põhikooliõpilased“ või „alaealine“. Kui teadustöös puudub vajadus andmesubjekte mingite tunnuste alusel eristada, võib kasutada üldisi sõnu, näiteks „uuringusse kaasatud isikud“ või „uuritavad“ (vt alaptk-d 2.10, 2.15 ja 2.16).

6. Milline on andmete kogumise viis?

Peamine küsimus on, kas andmeid kogutakse vahetult inimestelt endilt või kasutatakse juba varem muul eesmärgil kogutud ehk teiseseid andmeid. Teiseste andmete puhul tuleb kindlaks määrata, kust need pärinevad, millised on kokkulepped andmete valdajatega ja kuidas on tagatud andmete turvaline üleandmine uurijatele (vt alaptk 2.8).

Sõltumata andmete kogumise viisist tuleb inimestele anda teavet nende andmete töötlemise kohta (vt p 2.8.2).

7. Milline on töötlemise õiguslik alus?

Selleks, et isikuandmete töötlemine oleks seaduslik, peab alati esinema üks üldmääruses nimetatud õiguslik alus (vt alaptk 1.6). Teadusprojekti eri etappidel võivad olla eri õiguslikud alused, kuid samas etapis ei saa valida neist mitut. Enamasti on küsimus selles, kas isikuandmete töötlemine toimub inimese nõusolekul (vt alaptk 2.3) või muul õiguslikul alusel (vt alaptk 2.4).

8. Kus ja kuidas andmeid hoitakse?

Mõelda tuleb sellele, kus ja kuidas andmeid hoitakse, kes pääsevad neile juurde ning mis tingimustel. Näiteks on vaja otsustada, kas andmete hoidmise keskkonnaks on ülikooli server, töötajate arvutid,

pilveteenus vm ja kas see keskkond asub Euroopa Liidus või mõnes kolmandas riigis. Kui andmed on plaanis arhiveerida, on vaja aegsasti otsustada, millisel viisil ja kus neid säilitatakse (vt alaptk-d 2.2 ja 3.1).

9. Kui kaua isikuandmeid säilitatakse?

Eelnevalt tuleb kokku leppida, millisel kujul ja kui kaua uuringus kasutatud isikuandmeid säilitatakse. Teadusandmete kohta kehtib erand, mis lubab neid säilitada esialgse eesmärgi saavutamise ajast kauem, kuid mitte piiramatult. Tavapärane praktika on säilitada andmeid 5–10 aastat pärast projekti või uurimistöö lõppu, et oleks võimalik uuringu tulemusi kontrollida (vt alaptk 4.1).

Andmete varundamine ja pikaaegne säilitamine on tihedalt seotud teadusandmete haldamisega. Täpsemalt võib selle kohta lugeda Tartu Ülikooli raamatukogu õppematerjalist „Teadusandmete haldus ja publitseerimine“ ja andmehaldusplaani koostamise juhendist.

10. Milliseid turvameetmeid on plaanis kasutada?

Turvameetmed on nii tehnilist kui ka korralduslikku laadi. Tehnilised turvameetmed puudutavad andmete töötlemise seadmeid ja keskkondi. Korralduslikud turvameetmed on eelkõige töökord, füüsilised juurdepääsupiirangud (uksekaardid), ruumide ja seadmete lukustamine, andmehaldusplaan või isikuandmete töötlemise registreerimine. Turvameetmetena saab käsitada ka krüpteerimist, pseudonüümimist ja anonüümimist (vt alaptk-d 3.1, 3.3 ja 3.4).

11. Kellele on plaanis isikuandmeid edastada?

Nimetada tuleks kõik isikuandmete vastuvõtjad ehk isikud, kellele isikuandmeid edastatakse. Need võivad olla nii projektisisesed kui ka -välised asutused või isikud (vt alaptk 4.3).

12. Kas isikuandmeid edastatakse kolmandatesse riikidesse?

Kui isikuandmeid on plaanis edastada väljapoole Euroopa Liitu, kaasneb sellega kohustus tagada, et ka sihtriigis oleks piisav isikuandmete kaitse. Andmehaldusplaanis ja andmekaitsetingimustes tuleks kirjeldada ka kolmandatesse riikidesse edastavate andmete kooseisu ja kuju (vt alaptk 3.2).

2.2. Kui palju peab teadustöös isikuandmetega seonduvat dokumenteerima?

Enne teadustööga alustamist tuleks välja selgitada, milline isikuandmete töötlemise dokumentatsioon on plaanitavas teadustöös vajalik. Allpool on loetletud sellekohased võimalikud ja vajalikud dokumendid. Lisaks võib olla vaja isikuandmete töötlemist kirjeldada ka mujal, näiteks rahastajatele esitatavates taotlustes ja aruannetes.

2.2.1. Andmehaldusplaan

Andmehaldusplaan on vahend andmete ja nendega tehtava töö kirjeldamiseks. Selle koostamine algab kõige üldisematest vastustest küsimustele, kust ja kuidas plaanitakse andmeid saada, millised on nende tüübid ja kuidas need on seotud, milliseid andmevorminguid kasutatakse, milline on andmemaht, millist tarkvara kasutatakse, kus, kuidas ja kui kaua andmeid säilitatakse.

Andmehaldusplaan aitab kirjeldada andmeid, et muuta need avatud teaduse huvides leitavaks, juurdepääsetavaks, koostalitlusvõimeliseks ja taaskasutatavaks (*Findable*, *Accessible*, *Interoperable*, *Reusable*, FAIR-põhimõte). Ent lisaks saab plaani koostamisega tuvastada juba aegsasti isikuandmete töötlemisega kaasnevad võimalikud probleemid, samuti kohustused ja nõuded. Näiteks saab anda ülevaate sellest, milline osa andmetest on isikuandmed, kas töödeldakse eriliiki isikuandmeid, kas kasutatakse juba varem muul eesmärgil kogutud andmeid, kuidas tagatakse andmete konfidentsiaalsus ja terviklus või kellega andmeid jagatakse.

Kuigi ülikoolis ei ole üldist kohustust koostada iga uuringu jaoks andmehaldusplaan, on andmete süsteemne haldamine muutumas tavaks. Seda võivad nõuda ka uuringu rahastajad, näiteks programmi „Horisont 2020" toetuste, Euroopa Teadusnõukogu ja Eesti Teadusagentuuri grantide andjad. Kuna andmehaldusplaani loomisel moodustub süsteemne ülevaade kõigist andmetest, mida on plaanis koguda ja analüüsida, on see mõistlik ühendada isikuandmete töötlemise ülevaate kirjutamisega ja vajaduse korral eetikakomiteele esitatava taotluse koostamisega.

Loe lisaks

- Tartu Ülikooli raamatukogu andmehaldusplaani koostamise juhend
- Tartu Ülikooli raamatukogu teadusandmete haldamise kursus
- Tartu Ülikooli raamatukogu näited andmehaldusplaanidest
- Andmehaldusplaani koostamise tööriist

2.2.2. Andmekaitsetingimused

Andmekaitsetingimuste avaldamine on kohustuslik kõikidele asutustele, kes töötlevad isikuandmeid. Mahukamate teadusprojektide puhul võib olla tarvis koostada ka eraldi andmekaitsetingimused. Näiteks ülikooli andmekaitsetingimustes on esitatud üldinfo, kuid suuremahulise teadusprojekti raames toimuvat andmetöötlust tuleks eraldi kirjeldada. Rahvusvahelistes uuringutes seda üldjuhul ka tehakse.

Nõusolekupõhistes uuringutes esitatakse suur osa andmekaitsetingimustest ka informeeritud nõusoleku lehel. Kuna läbipaistvuspõhimõtte kohaselt peab isikuandmete töötlemist puudutav teave olema inimestele alati kättesaadav ja lihtsasti leitav, võiks sama teabe avaldada ka teadusprojekti või vastutava töötleja veebilehel (vt alaptk-d 2.7).

Loe lisaks

- Andmekaitse Inspektsiooni isikuandmete töötleja üldjuhendi lisa 3 „Andmekaitsetingimuste kontrollküsimustik"
- Tartu Ülikooli andmekaitsetingimused

2.2.3. Ülevaade isikuandmete töötlemisest

Isikuandmete töötlemise ülevaate koostamine on nii vastutava kui ka volitatud töötleja kohustus, mis tuleneb üldmääruse artiklist 30[3]. Üldjuhul ei ole ülevaate koostamine iga uuringu või projekti jaoks eraldi

[3] Üldmääruse artiklis 30 kasutatud väljendi *isikuandmete töötlemise toimingute registreerimine* asemel eelistatakse Eestis väljendeid *isikuandmete töötlemise ülevaade*, *ülevaade isikuandmete töötlemisest* ja *isikuandmete töötlemisülevaade.* Kaht esimest on kasutatud ka siin juhendis.

põhjendatud ega vajalik. Samas ei pruugi ülikool tegelikult teada, kuidas täpsemalt isikuandmeid mõnes mahukas uuringus või projektis töödeldakse. Samuti võib olla vastutus isikuandmete eest jagunenud arvukate teadusasutuste vahel. Seda arvesse võttes võib olla siiski vajalik koostada ülevaade isikuandmete töötlemisest ka ühe teadusprojekti jaoks, eriti kui selles töödeldakse tundlikke andmeid või kasutatakse suurema riskiga andmetöötlusmeetodeid.

Loe lisaks

Andmekaitse Inspektsiooni isikuandmete töötleja üldjuhendi 4. peatükk „Isikuandmete töötlemisülevaade“

2.2.4. Eetikakomitee kooskõlastus

Mitmes Eesti seaduses on antud eetikakomiteedele ülesanne hinnata kavandatava teadustöö vastavust andmekaitsenõuetele. Eetikakomitee kooskõlastus on olenevalt teadustööst kohustuslik või vabatahtlik. Kooskõlastustaotluses tuleb kirjeldada muu hulgas, milliseid isikuandmeid, millisel õiguslikul alusel, kuidas ja kui kaua töödeldakse (vt ka alaptk 2.13).

2.2.5. Andmekaitsealane mõjuhinnang

Kui teadusuuringu andmetöötlus kujutab endast suurt ohtu inimeste õigustele ja huvidele, saab neid kaitsta andmekaitsealase mõjuhinnanguga, mis on vastutavale töötlejale kohustuslik. Kui teadlasele tundub, et plaanitava teadustöö jaoks võib mõjuhinnang olla vajalik, tuleks ühendust võtta andmekaitsespetsialistiga.

Koostööprojektide puhul tuleks eraldi kokku leppida, millised partnerid vastutavad mõjuhinnangu tegemise eest ja kuidas teisi partnereid sellesse kaasatakse. Lisaks tasub arvestada, et eri Euroopa Liidu riikides tehakse mõjuhinnangut eri viisidel. Rahvusvaheliste projektide puhul oleks seega mõistlik eelnevalt arutada ja kokku leppida, millisel viisil ja kes mõjuhinnangu koostab.

Andmekaitsealane mõjuhinnang on spetsiifiline kohustus, mis ei tähenda, et teist laadi riskide hindamine ei ole vajalik. Sõltuvalt olukorrast võib olla vajalik ka andmeturbe- või eetiliste riskide hindamine (vt ka alaptk 2.14).

2.2.6. Informeeritud nõusolek

Nõusolek on üks võimalik õiguslik alus isikuandmete töötlemiseks teadustöös. Informeeritud nõusoleku lehel peab sisalduma kõige olulisem teave isikuandmete töötlemise kohta. Mõnikord tuleb luua samast infolehest mitu versiooni, näiteks üks täiskasvanutele ja teine lastele. Samuti võib olla vajalik informatsiooni tõlkimine eri keeltesse.

Informeeritud nõusoleku leht koos inimese nõusolekuga on ametlik dokument, mida tuleb nõuetekohaselt hoida. Teadlasel võib olla vajalik tõendada andmesubjektilt saadud nõusolekut, kui näiteks inimene vaidlustab enda andmete töötlemise. Lisaks võivad informeeritud nõusoleku lehega tutvumist nõuda eetikakomiteed või rahastajad hindamaks, kas see vastab nõuetele.

Nõusolekut on võimalik tagasi võtta. Ka tagasivõtmine tuleb dokumenteerida (vt järgmine alaptk).

2.3. Milline peab olema inimeselt küsitav nõusolek?

Nõusoleku eesmärk on anda andmesubjektile võimalikult suur kontroll oma andmete üle. Seepärast ei sobi see õiguslikuks aluseks selliste teadusuuringute puhul, kus inimese võimalused oma andmete töötlemist kontrollida on väga piiratud.

Üldmääruse kohaselt tunnistatakse uuringus osalemise nõusolek kehtivaks ainult siis, kui seda on aktiivselt väljendatud ja selgelt kinnitatud (nt sõnaga „jah", linnukese tegemisega, allkirja lisamisega). Seega peab andmesubjekt andma ise **vabatahtlikult**, **teadlikult**, **konkreetselt** ja **ühemõtteliselt** nõusoleku teda puudutavate isikuandmete töötlemiseks (*opt-in*). Vastupidine olukord, kus isikuandmete kogumisel eeldatakse nõusolekut vaikimisi ja sellest loobumiseks peab osaleja midagi tegema (*opt-out*), on keelatud ja vastuolus üldmäärusega.

Valiku näitlikke nõusolekuvorme leiab Tartu Ülikooli siseveebist.

Loe lisaks

- Euroopa Andmekaitsenõukogu suunis 05/2020 määruses (EL) 2016/679 sätestatud nõusoleku kohta
- Andmekaitse Inspektsiooni isikuandmete töötleja üldjuhendi lisa 2 „Nõusoleku kontrollküsimustik"

2.3.1. Nõusolek peab olema vabatahtlik

Inimest ei tohi mõjutada nõusolekut andma. Nõusolek ei ole vabatahtlik, kui inimesel puudub tegelik valikuvabadus. Lubatud ei ole kingituste, raha ega muude hüvedega meelitamine, veenmine ega survestamine.

Nõusolekut ei peeta vabatahtlikuks, kui

- nõusoleku andja ja küsija on selgelt ebavõrdses võimu- või sõltuvusvahekorras, näiteks kui nõusolekut küsib õppejõud üliõpilaselt või tööandja töötajailt;
- selle andmine on mingi teenuse osutamise või hüve või võimaluse kasutamise eeldus. Näiteks erialastel konverentsidel või seminaridel ei saa seada osalemise tingimuseks isikuandmete töötlemisega nõustumist (piltide või ülekande tegemine), ilma milleta ei pääse üritusele. Sama kehtib avaandmete hoidlate puhul: avaandmetele juurdepääsu võimaldaval veebilehel ei tohi olla näiteks küpsistega nõustumine vajalik selleks, et andmetele ligi pääseda. Teadustöö puhul on siiski üsna keeruline ette kujutada olukorda, kus andmete kogumine on seotud mõne andmesubjektile huvipakkuva tegevuse või teenusega;
- nõusoleku tagasivõtmisega kaasnevad inimesele kahjulikud tagajärjed. Seega peab tagama ühtviisi nii nõusoleku andmise kui ka tagasivõtmise vabatahtlikkuse.

2.3.2. Nõusolek peab olema teadlik

Teadlikkus tähendab, et inimene teab ja mõistab, millega ta nõustub. Üldmääruse kohaselt peab nõusolekuks antav teave olema selges ja lihtsas keeles. Vältida tuleb keerulisi teadus- või õigustermineid.

Nõusolekuvormil tuleb anda inimesele teavet tema andmete töötlemise kohta. Kui seda ei tehta, ei saa tema antud nõusolekut pidada teadlikuks ja see ei kehti. Nõusolekus tuleb selgitada kogu andmetöötlust

algusest lõpuni (andmete kogumine, analüüsimine, edastamine, säilitamine). Paratamatult tähendab see, et nõusoleku küsimiseks tuleb esitada inimesele *kogu* üldmääruses nõutud teave:

- vastutava töötleja ja tema esindaja nimi ning kontaktandmed;
- andmekaitsespetsialisti kontaktandmed;
- isikuandmete töötlemise eesmärk ja õiguslik alus;
- isikuandmete vastuvõtjad ehk need, kellele on kavas andmeid edastada;
- isikuandmete säilitamise tähtaeg;
- õigus nõusolek tagasi võtta ja muud õigused oma andmete suhtes;
- teave andmete edastamise kohta kolmandatesse riikidesse;
- teave automatiseeritud otsuste ja füüsilise isiku profiilianalüüsi kohta.

Teadlikkus eeldab seega kompromissi kahe vastandliku huvi vahel: ühest küljest peab teavet olema piisavalt, et lugeja saaks ülevaate isikuandmete töötlemisest, teisest küljest peab teave olema lihtne ja selge, et tagada teabest arusaamine.

Teavet võib anda igal kujul. Peale kirjaliku teksti võib kasutada ka näiteks videot, helisalvestist, animatsiooni, pilte või ikoone. Hea lahendus on teha teabest mitu versiooni – üks lühem ja lihtne, teine mahukam, põhjalikum ja tekstipõhine.

2.3.3. Nõusolek peab olema konkreetne ja ühemõtteline

Konkreetsus tähendab, et isikuandmete töötlemise eesmärk on selgelt esitatud. Et aga teadustöös võib eesmärgi täpne sõnastamine olla keeruline, sest sageli ei ole planeerimist alustades päris täpselt teada, milliseid andmeid ja kuidas töödeldakse ning missugused on nende hilisemad kasutusviisid, on tehtud mõningane mööndus: teadustöö eesmärgi sõnastus peaks olema nii konkreetne kui sel hetkel võimalik. Eesmärgi väiksemat konkreetsust aitavad heastada suurem läbipaistvus kogu teadustöö vältel (näiteks teavitatakse andmesubjekte pidevalt projekti käigust) või korduv nõusoleku küsimine (näiteks teatud uuringuetappide järel palutakse uut nõusolekut).

Ühemõttelisus on tihedalt seotud läbipaistvuspõhimõttega – see tähendab, et nõusolek peab olema üheti mõistetav ja selge sõnastusega, selles ei tohi olla eksitavaid ja segaseid väiteid. Näiteks mitme eesmärgi puhul tuleb nõusolekuvorm koostada selliselt, et andmesubjekt saab valida, millistega neist ta nõustub ja millistega mitte (vt ka alaptk 2.12).

2.3.4. Isikuandmete töötlemise nõusolek peab selgelt eristuma muudest nõuetest ja nõusolekutest

Teadustöös kasutatavate isikuandmete töötlemise nõusolek on kohati väga sarnane uuringus osalemise nõusolekuga. Seega peab nõusoleku andja mõistma, et näiteks ravimi kliinilises uuringus osalemise nõusolek ei tähenda automaatselt nõustumist isikuandmete töötlemisega. Selle asemel tuleb inimesel anda kaks nõusolekut: üks isikuandmete töötlemiseks ja teine uuringus osalemiseks. Siiski on need omavahel seotud ja kui inimene näiteks andmetöötlusega ei nõustu, ei saa ta uuringus osaleda.

Lisaks tasub meeles pidada, et teadusuuringus osalemise nõusolek peab kajastama ka sellist teavet, mida isikuandmete töötlemise nõusolek ei eelda. Osalemisnõusolekus peavad olema kirjas teadustöö eesmärk ja korraldus, seotud teadlased, teadusasutused ja rahastajad, teadustöö eeldatav ühiskondlik kasu ja võimalik kahju ning nende kaalumise kirjeldus, töö tulemuste võimalik kasutusviis, inimesele kaasnevad riskid ja kavandatud meetmed nende vähendamiseks.

2.3.5. Nõusoleku andmist peab suutma tõendada

Nõusolekuvormi kohta ei ole selgeid nõudeid peale selle, et see peab olema tõendatav ehk dokumenteeritud. Seepärast tasub see võtta kirjalikult. Sobib ka suuline nõusolek, kui see on teadlasel salvestatud ja seda saab taasesitada.

Nõusoleku andmist ei pea tingimata allkirjaga kinnitama, mistõttu sobib selleks ka e-kiri. Samas tuleb suuta tõendada, et andmesubjekt on ise nõusoleku andnud. Kui isikuandmete töötlemisel tekib probleeme ning teadusasutus ei suuda tõendada, et tal on selleks nõusolek, võib Andmekaitse Inspektsioon käsitada seda ebaseadusliku töötlemisena.

Ka dokumenteeritud nõusolekud on käsitletavad isikuandmetena. Lisaks on need ülikooli ametlikud töödokumendid, mille hoidmise aeg, viis ja koht on kokku lepitud asutuse asjaajamiskorras. Üldiselt tuleb neid säilitada andmetöötluse lõpuni.

2.3.6. Töötlemine peab piirduma nõusolekus kirjeldatuga

Nõusolek kehtib vaid selles kirjeldatud tingimustel. Kui inimest mõnest töötlustoimingust nõusolekuvormil ei teavitata, puudub selliseks töötlemiseks õiguslik alus. Kui töötlemise laad või ulatus teadustöö käigus märgatavalt muutub, tuleb saada isikuandmete jätkuvaks töötlemiseks uus nõusolek.

Jätku-uuringu puhul on vaja muretseda uue andmekogumise ajal uus nõusolek, isegi kui inimest algse nõusoleku küsimise ajal jätku-uuringust teavitati.

2.3.7. Nõusolekut peab olema lihtne tagasi võtta

Inimesel peab olema võimalus nõusolek tagasi võtta ja see ei tohiks olla põhjendamatult keeruline. Vastasel korral on nõusolek tühine ja kogu isikuandmete töötlemine ebaseaduslik.

Kui uuringus osaleja tahab oma nõusoleku tagasi võtta, tuleb paluda tal see esitada digitaalselt allkirjastatud avaldusena või muul isikut tuvastada võimaldaval viisil. Andmete töötlejal tuleb veenduda, et see, kes nõusoleku tagasi võtab, oma sama isik, kes on selle andnud.

Tagasivõtmise teemaline suhtlus ei tohiks piirduda ainult nõusolekust loobumisega, vaid hea tava on ka selgitada andmesubjektile, mis saab tema andmetest pärast nõusoleku tagasivõtmist. Näiteks tuleb üle korrata, et nõusoleku kehtivuse ajal tehtud andmetöötlus oli õiguspärane ja seda ei saa tagasi võtta. Andmetöötlus lõpeb hetkest, kui isik oma nõusoleku tagasivõtmisest teada annab.

2.4. Mida pidada silmas, kui isikuandmeid töödeldakse ilma inimese nõusolekuta?

IKS-i § 6 kohaselt võib teadustöös töödelda isikuandmeid teatud juhtudel ka ilma inimese nõusolekuta ja kasutada mõnda muud õiguslikku alust, näiteks avalikes huvides ülesande täitmiseks. Kahjuks ei ole kuigi palju selgust olukordadeks, kui teadustöö õiguslik alus on avalikes huvides ülesanne, mistõttu ei saa praegusel ajal anda väga konkreetseid soovitusi nõusolekuta uuringuteks. Ent allpool on esitatud siiski paar üldist nõuannet, millega tuleks avalikes huvides ülesande täitmisel ilma nõusolekuta uuringute puhul kindlasti arvestada.

2.4.1. Andmed tuleb pseudonüümida või täita tuleb IKS-i lisanõudeid

IKS-i § 6 lg 1 alusel võib teadusuuringu eesmärgil ilma inimese nõusolekuta tema isikuandmeid töödelda eelkõige pseudonüümitult või samaväärset kaitset võimaldaval kujul. Esmajoones puudutab

pseudonüümimistingimus teiseseid uuringuid, näiteks kui teadlane soovib uuringus kasutada avaliku andmekogu teavet või varem muul eesmärgil kogutud isikuandmeid ja õiguslik alus on avalikes huvides ülesanne.

Erandina on lubatud töödelda ilma nõusolekuta ka isikustatud kujul isikuandmeid, kui on täidetud kõik IKS-i § 6 lg-s 3 nimetatud tingimused.

- **Teadustöö eesmärk on saavutatav vaid isikustatud kujul andmetega**

Kui teadustöö eesmärk on näiteks järelduste tegemine konkreetsete isikute kohta, huvipakkuv teadmine võib olla väga lähedalt seotud kindlate inimestega või teadustöö võib puudutada väga otseselt teatud isikute huve ja õigusi, on võimalik kasutada ka isikustatud andmeid. Teadlane peab isikustatud andmete kasutamise vajadust alati põhjendama, selgitades ühtlasi, miks ei saa plaanitavat teadustööd teha isikute nõusolekul.

- **Teadustöö suhtes esineb ülekaalukas avalik huvi**

Avalik huvi võib kaasneda nii rakenduslike kui ka alusuuringutega. Avalikes huvides oleva ülesande täitmine tähendab, et plaanitaval uuringul on teaduslik või ühiskondlik väärtus, mida teadlane peab põhjendama. Avalik huvi peab olema ülekaalukas – kui näiteks teadustöö riivab olulisel määral inimeste õigusi ja vabadusi, saab seda õigustada väga suure avaliku huviga.

- **Teadustööga ei kahjustata andmesubjekti õigusi**

Teadlane peab hindama võimalikku kahju andmesubjekti õigustele. Kui kahju ei esine üldse, on plaanitav teadustöö suure tõenäosusega lubatud. Kui esineb siiski oht õigusi kahjustada, tuleks võtta leevendavaid meetmeid või leida muu viis teadustöö tegemiseks.

Enamasti võib eeldada, et kui täidetud on kõik isikuandmete kaitse seaduse § 6 kriteeriumid ja esitatud põhjendused on veenvad, on täidetud tingimused, mis võimaldavad määrata õiguslikuks aluseks avalikes huvides ülesande.

IKS-i § 6 lg 3 kohase põhjenduse ja hinnangu koostamine on teadlase või teadusasutuse ülesanne. Kui isikustatud kujul isikuandmed on eriliiki, tuleb saada ka eetikakomitee kooskõlastus.

2.4.2. Viidata tuleb õigusakti sättele

Avalikes huvides olev ülesanne peab tulenema õigusaktist. Seega tuleks läbipaistvuse huvides alati selgitada, milles seisneb plaanitava teadustööga seotud avalik huvi, ja viidata ka õigusaktile, mis seda avalikku ülesannet täpsustab.

Mõnel avalikul teadusasutusel on teadustöö ülesanne täpsustatud eraldi õigusaktis, mille alusel asutus töötab, ja sel juhul on võimalik viidata konkreetsele sättele. Teinekord võib ainsaks õigusaktiks olla isikuandmete kaitse seadus, mis aga ei garanteeri, et iga plaanitava teadustöö suhtes esineb automaatselt avalik huvi. Sel juhul peavad teadustöö tegijad andma lisapõhjendusi või -selgitusi selle kohta, milles avalik huvi seisneb.

2.5. Kuidas tagada isikuandmete seaduslik töötlemine?

Isikuandmete töötlemine teadustöös on seaduslik, kui selleks on olemas õiguslik alus, järgitud on üldmääruse ja Eesti isikuandmete kaitse seaduse nõudeid ning nendest tulenevaid andmekaitsepõhimõtteid. Lisasoovitusi leiab veel Euroopa Andmekaitsenõukogu suunisest 4/2019 üldmääruse artikli 25 „Lõimitud andmekaitse ja vaikimisi andmekaitse“ kohta. Allpool on suunise põhjal selgitatud, kuidas järgida teadustöös seaduslikkuse põhimõtet.

2.5.1. Õiguslik alus määratakse enne isikuandmete töötlemisega alustamist

Teadusuuringute puhul on peamine küsimus see, kas inimese isikuandmeid töödeldakse tema nõusolekul või mitte. Isikuandmete nõusolekuta töötlemine vajab alati põhjendamist ja muud sobivat õiguslikku alust, näiteks lepingut, seadusest tulenevat kohustust või avalikes huvides ülesande täitmist (vt ka alaptk 1.6).

Näide

Teadlane uurib sotsiaalmeedias leiduvat avalikku materjali, mida inimesed on enda kohta postitanud. Kuna teadlase teada ei ole tavaks meedias avaldatud materjalide analüüsimisel inimestelt nõusolekut küsida, ei plaani ka tema seda teha. Mõni aeg hiljem, kui andmed on juba kogutud, avastab teadlane, et inimesed on postituste kommentaaride põhjal tuvastatavad, sest tekstiotsinguga leiab nad üles. Isegi kui ta kogutud andmeid ei avalda, on olnud siiski tegemist nõusolekuta isikuandmete kogumise ja analüüsiga, mis eeldanuks õiguslikku alust. Teadlane võib küll leida, et selleks on avalikes huvides olev ülesanne, kuid selles tuleks veenduda enne andmete kogumisega alustamist.

2.5.2. Määrata tuleb kõige asjakohasem õiguslik alus

Kuna üldmäärus võimaldab õigusliku aluse puhul teatud paindlikkust, ei pruugi mõnikord olla üheselt selge, milline õiguslik alus on teadusuuringu puhul võimalik ja õige.

Õiguslik alus peab olema selgelt sõnastatud ja see ei tohi inimest eksitada. Inimesele ei tohi jääda muljet, et temalt on küsitud nõusolekut, kui tegelikult ei ole tema nõusolek isikuandmete töötlemise õiguslik alus. Kui inimene võtab oma nõusoleku tagasi, ei või teadusasutus jätkata tema andmete töötlemist samal eesmärgil muudel alustel, väites näiteks, et teadustöö tegemine on avalikes huvides olev ülesanne ja seega võib isikuandmeid töödelda ka nõusolekuta.

Näide

Teadlane küsib teadusuuringuks andmeid avalikust andmekogust. Avalik asutus, kes andmeid valdab, esitab teadlasele pseudonüümitud andmestiku, kus identifikaatorid ehk inimese otsest või kaudset tuvastamist võimaldav teave on krüpteeritud. Teadlane saab aru, et tegemist on pseudonüümitud andmetega, mille töötlemiseks on vaja õiguslikku alust. Kuna selles avalikus andmekogus saab iga Eesti kodanik määrata enda eelistuse andmete väljastamiseks muudel eesmärkidel, sh teaduslikul eesmärgil, peab teadlane õiguslikuks aluseks inimese nõusolekut, sest andmete väljastamine põhineb inimese vabal tahtel. See hinnang on aga ekslik. Andmekogus märgitud valik on vajalik selleks, et avalikul asutusel oleks õigus andmeid teadusuuringuks välja anda, kuid selline nõusolek ei vasta üldmääruse tingimustele – näiteks pole selge, kuidas saab inimene enda nõusoleku tagasi võtta. Lisaks ei ole teadlane inimestele nõusoleku küsimiseks vajalikku teavet esitanud.

2.5.3. Eristada tuleb teadustööga kaasnevat tegevust, mis võib vajada omaette õiguslikku alust

Iga töötlemistoiming tuleb eesmärgi ja õigusliku aluse põhjal selgelt eristada. Kui väiksemamahulisel uuringul on vaid üks eesmärk (teadusuuringu eeldatav tulemus) ja üks õiguslik alus (nõusolek), on selle soovituse täitmine lihtne. Mahukate, aastatepikkuste teadusprojektide raames võib aga eesmärke olla rohkem ja sel juhul tuleb iga eesmärk siduda õigusliku alusega.

Kui samas teadusuuringus on plaanis koguda andmeid vahetult inimestelt ning ühendada need juba varem kogutud ja mujal asuda võivate andmetega, tuleks õiguslik alus määrata mõlemale toimingule eraldi, isegi kui need täidavad sama eesmärki.

Näide

Teadustöös kasutatakse isikuandmeid, mida ei ole võimalik anonüümida ilma nende kvaliteeti kahjustamata, kuid soov on neid säilitada teadusandmete repositooriumis ja muuta teistele teadlastele kasutatavaks. Kuigi avatud teadus on hea ja oluline, ei ole isikuandmete jagamine teiste teadlastega konkreetse teadustöö eesmärkide saavutamiseks vajalik. See on juba iseseisev eesmärk. Üks võimalik lahendus on küsida uuringus osalejatelt lisanõusolekut. Sel puhul valivad nad, kas lubavad enda andmeid kasutada vaid konkreetses uuringus või ka tulevastes teadustöödes.

2.5.4. Inimestele on antud võimalikult suur otsustamisvabadus

Teadustöö planeerimisel tuleks anda andmesubjektile võimalus valida, kuidas ta soovib uuringus osaleda ja mil viisil tema andmeid kasutatakse. See, kui palju saab jätta inimesele autonoomiat ja otsustusvabadust, sõltub konkreetsest uuringust. Näiteks eksperdiga tehtava intervjuu puhul on võimalik määrata, kuidas tema ja tema öeldu on avaldatud tekstis seostatud: kas kasutatakse eksperdi nime või pseudonüümi või viidatakse tema töökohaks olevale asutusele.

Kui valida on mitme õigusliku aluse vahel, tuleks võimalusel eelistada nõusolekut. Vaid juhtudel, kus nõusoleku küsimine ei ole võimalik või see takistab teadustöö eesmärkide täitmist, võib kaaluda muid õiguslikke aluseid, kuid ka sellisel juhul peaks andmete valdaja tagama inimesele võimalikult suure autonoomia – näiteks valiku keelata oma andmete kasutamist muudel eesmärkidel.[4]

2.6. Kuidas tagada isikuandmete õiglane töötlemine?

Allpool on esitatud Euroopa Andmekaitsenõukogu suunises 4/2019 üldmääruse artikli 25 „Lõimitud andmekaitse ja vaikimisi andmekaitse“ kohta loetletud soovitused koos lühiselgitusega, kuidas järgida teadustöös isikuandmete töötlemise õigluspõhimõtet.

2.6.1. Isikuandmete töötlemine on kooskõlas inimese ootustega

Teadusuuringus kasutatavate isikuandmete töötlemise kirjeldus peab olema võimalikult täpne ja hõlmama kõiki asjaolusid, mille puhul võib aimata, et need on inimeste jaoks olulised või võivad tekitada pahameelt. Teadusuuringu ja isikuandmete töötlemise kohta antav teave ei tohi olla eksitav ega tekitada andmesubjektis põhjendamatuid ootusi.

[4] Sellist võimalust pakub näiteks e-rahvastikuregister, kus igal inimesel on võimalik piirata enda aadressi väljastamist eraettevõtetele, kuigi andmete väljastamine ei põhine isiku nõusolekul.

Näide

Uuringus osalejale selgitatakse, et tema andmed ja intervjuu sisu on konfidentsiaalsed ja keegi peale uuringu korraldaja neid ei näe. Pärast uuringu lõppu tutvub osaleja avaldatud lõpptulemustega ja avastab, et temaga tehtud intervjuu katke on publitseeritud: kuigi tema nime ei ole avaldatud, tunneb ta oma sõnad ära. Inimene on pettunud ja annab sellest ka töö autorile teada, sest tema oli aru saanud, et intervjuu jääb täiesti konfidentsiaalseks. Teadlane aga selgitab, et see on üldlevinud akadeemiline tava, et kvalitatiivsete analüüside puhul tsiteeritakse katkeid intervjuudest.

Selline olukord võib olla uuritava suhtes ebaõiglane, kuna tema ei pea akadeemilist tava tundma. Teadlase tegevus ei ole küll andmekaitse vaatest ebaseaduslik, kuid näitlikustab, kuidas inimese ootused ja teadlase eeldused võivad erineda. Selliseid olukordi aitaksid ennetada lisaselgitused teadustöö eesmärkide ja andmete töötlemise kohta.

Väiksemate homogeensete valimitega kvalitatiivsete sotsiaalteaduslike uuringute puhul on välja kujunenud ka tava uuringu tulemusi enne avaldamist uuritavatele näidata – see aitab saada tagasisidet ja mõista paremini uuringusse kaasatute ootusi. Ühtlasi parandab see teadustöö läbipaistvust ja tagab, et inimeste ootused kattuvad teadustöös tehtuga.

2.6.2. Vastutava töötlejaga peab saama vahetult suhelda

Võimalus igal ajal teadustöö tegijatega ühendust võtta aitab kindlustada isikuandmete läbipaistva, õiglase ja usaldusväärse töötlemise. Keerulisem võib see olla juhul, kui andmete kogumine on delegeeritud volitatud töötlejatele (näiteks küsitlusettevõttele) ja nende töötajatele, kes võib-olla ei teagi kuigi üksikasjalikult uuringu eesmärke, andmete töötlemise tingimusi ega muud olulist teavet, mida inimesed võivad küsida. Sel juhul peaks uuringu eest vastutav teadusrühm lisama teabe, kuidas uuringu tegijatega ühendust võtta, ja oma kontaktandmed. Lisaks võib avaldada vastutava töötleja andmekaitsespetsialisti kontaktandmed.

2.6.3. Välditud on diskrimineerimist isikuandmete töötlemisel

Mittediskrimineerimise põhimõte on universaalne ega puuduta ainult andmekaitset. Kellegi diskrimineerimisel võib kogu andmetöötlus muutuda ebaõiglaseks ja selle kaudu ebaseaduslikuks.

Teadusuuringute puhul pole siiski alati kuigi selge, millist töötlemist pidada diskrimineerivaks. Teatud ühiskonnarühmad võivad olla uuringutes ala- või üleesindatud sõltuvalt sellest, kuivõrd lihtne või mugav on neilt andmeid koguda. Niisugune diskrimineerimine võib halvendada teadustöö kvaliteeti, kuna kallutatud valimi põhjal tehtud järeldused ei pruugi olla valiidsed, eriti kui pidada neid kogu ühiskonna läbilõikeks. Seepärast on tavapärane, et esindusliku valimi saamiseks esitatakse uuringusse kaasatutele lisatingimusi, mille alusel eelistatakse teatud osalejaid teistele. Näiteks on lävepakuküsitluste puhul tavaks esimesena küsitleda noorimat kodus olevat meest, kuna seda valimisegmenti on küsitlustega kõige raskem tabada. Valimipõhiseid kriteeriume võib pidada mittediskrimineerivaks, kuna uuringus osalemisega ei kaasne inimestele hüvesid.

2.6.4. Välditud on inimeste vajaduste või haavatavuse ärakasutamist

Inimestega ei või teadustöö eesmärgil manipuleerida ega neid ära kasutada. Teadusuuringute puhul on see oluline just vabatahtliku osalemise tagamisel, kuna igasugune mõjutamine piirab inimese võimalusi teha otsuseid iseseisvalt. Eriti tähelepanelik tuleks olla olukorras, kus uuritavad inimesed ei ole täiesti vabad või ei taju, et nende tegevust ja käitumist uuritakse.

Haavatavuse ja ekspluateerimise teema on seotud tihedalt teaduseetikaga. Andmekaitse vaatest on kõigil inimestel enda kohta käivate andmete suhtes võrdsed õigused, sõltumata nende haavatavusest. Ainsaks erandiks on lapsed, kelle andmete töötlemisel tuleb erilist tähelepanu pöörata nii nende õigustele kui ka sellele, et laste huve ei kahjustataks.

2.6.5. Välditud on võimupositsiooni

Võimusuhet tuleb arvesse võtta vabatahtlikkuse hindamisel, sest kõrgemal positsioonil inimese mõjuväljas võib uuringusse kutsutu tajuda sundi enda isikuandmeid avaldada. Seetõttu võib olla ebaõiglane olukord, kus õppejõud kaasab uuringusse enda õpetatava kursuse üliõpilased, kelle eksamitulemused sõltuvad temast. Samuti võib vabatahtlikkusega olla probleeme juhul, kui arst soovib uuringusse värvata enda patsiente või asutuse juht enda töötajaid.

2.6.6. Isikuandmete töötlemine on eetiline

Ebaõiglaseks võib pidada ka sellist isikuandmete töötlemist, mis ei ole kooskõlas uuringuvaldkonna eetiliste põhimõtetega. Teaduseetika olulisust näitab eriliiki isikuandmete töötlemisel nõutav eetikakomitee kooskõlastus. Tuleks arvestada, et teaduseetika põhimõtete rikkumisega võib halvemal juhul kaasneda andmekaitsealane vastutusele võtmine.

2.7. Kuidas tagada isikuandmete läbipaistev töötlemine?

Läbipaistvus tähendab, et andmesubjekt teab ja mõistab, kuidas tema isikuandmeid teadustöös kasutatakse. Läbipaistvuse saavutamiseks peab uuringus osalejal olema võimalik saada teavet nii teadustöö eel kui ka isikuandmete töötlemise ajal. Teisalt on antava teabe kogus ja kvaliteet hinnanguline ning seda, kui läbipaistev peab teadustöö olema, ei ole kuigi põhjalikult ette kirjutatud.

Allpool on kommenteeritud Euroopa Andmekaitsenõukogu suunist 4/2019 üldmääruse artikli 25 „Lõimitud andmekaitse ja vaikimisi andmekaitse“ kohta lühiselgitusega selle kohta, kuidas tagada teadustöö puhul võimalikult suur läbipaistvus.

2.7.1. Antav teave on selge, arusaadav ja asjakohane

Andmesubjekti teavitamisel tuleb vältida keerulist sõnastust ja lausestust, erialatermineid, mitmetimõistetavust ja eksitamist. Antav teave ei tohiks olla mahukas tekstimass, mida on raske läbi lugeda. Hea lahendus on esitada teavet mitmeastmeliselt: tehakse lühikokkuvõte kõige olulisemast, kuid selle juures on viited lisateabele, kust saab põhjalikuma ülevaate isikuandmete töötlemisest.

Teabe esitamisel peab lähtuma sihtrühmast. Näiteks võib olla vajalik esitada sama teave lastele ja täiskasvanutele erineva arusaadavusastmega. See tingib mõnes olukorras teabe lihtsustamise.

2.7.2. Teabe esitamiseaeg ja kanal on sobivad

Teavitamisel tuleb kasutada eri võimalusi ja arvestada andmesubjekti vajadustega. Teave peab olema lihtsasti leitav.

- Kui isikuandmeid kogutakse intervjuu käigus, on sobivaim teavitusaeg vahetult intervjuu eel.
- Kui inimesele saadetakse andmekaitsealane teave koos kutsega uuringule, peaks seesama teave olema kättesaadav ka uuringukohas enne isikuandmete kogumisega alustamist. Lisaks teabelehele võiks isikuandmete töötlemise info olla ka projekti või ülikooli veebilehel.

- Kui teadlane kogub andmeid mõne sotsiaalmeedia keskkonna vahendusel, peaks inimesi teavitama lisaks muudele kanalitele ka sellesama sotsiaalmeediaplatvormi kaudu.
- Peamine teave võiks olla masinloetaval kujul, kuid üldmääruse kohaselt võib inimesele teabe edastada ka suuliselt, kui ta seda soovib.

2.7.3. Kasutatavate algoritmide kohta antakse teavet

Üldmääruses on eraldi käsitluse all isikuandmete automatiseeritud töötlemine, mille tulemusena tehakse inimese või tema käitumise kohta otsus, mis põhineb üksnes automatiseeritud töötlemisel ning avaldab inimesele suurt mõju (toob kaasa õiguslikke või võrreldavalt olulisi tagajärgi). Näiteks on lubamatu teha automaatsel profiilianalüüsil põhinevaid värbamis- ja finantsotsuseid.

Kui teadustöös on kavas kasutada automatiseeritud töötlemist, näiteks masinõppe algoritme, mis teeb otsuseid või järeldusi inimese või tema käitumise kohta, tuleb seda inimesele selgitada. Selgitatavus on tehisintellekti kasutamise puhul läbipaistvust toetav eetiline põhimõte, mis eeldab, et iga inimsekkumiseta otsus on teadustöös osalejale arusaadav. Samuti tuleb talle öelda, mis on sellise lahenduse eeldatav tulemus ja milleks seda kasutatakse.

Siiski ei piirata üldmääruses automatiseeritud andmetöötluse kasutamist üldiselt. Masinõppemeetodid, mille eesmärk on leida suurte andmehulkade ja arvukate tunnuste põhjal olulisi seoseid, ei too kaasa õiguslikke tagajärgi ega ole kuidagi piiratud. Sama kehtib üldistatud andmete põhjal statistiliste järelduste tegemise kohta, millega ei kaasne kohustust anda teavet iga statistilise arvutuse aluseks oleva algoritmi kohta.

Seega sõltub teavitamisvajadus eelkõige töötlemise mõjust inimesele ja seda tuleb hinnata teadustööpõhiselt.

2.7.4. Kaasvastutuse korral on selgelt eristatud, mille eest ja mil määral keegi vastutab

Kui samade töötlustoimingute eest vastutab mitu töötlejat, peavad nende ülesanded olema selgelt jagatud. Teadusasutuste kaasvastutus tuleb alati kokku leppida eraldi lepinguga, kuhu saab kirja panna, mil määral nad vastutavad ühiselt ja mil määral eraldi.

Näide

Kui üleeuroopalises projektis vastutab ülikool isikuandmete kogumise ja esmase töötlemise eest, ent koondanalüüsiks saadetakse kõigi riikide andmed kaasvastutavale projektipartnerile, tuleb sellist vastutuse jaotust uuritavale selgitada. Sel juhul ta teab, milline teadusasutus millises etapis tema andmete kasutamist kontrollib ja kelle poole tal tuleb oma õiguste teostamiseks pöörduda. Kui andmesubjekt ei saa aru, kes nimekirjas olevatest arvukatest teadusasutustest ikkagi tema andmetele ligi pääseb ja neid hoiab, ei ole see teave piisavalt läbipaistev.

2.8. Mida pidada silmas teiseste isikuandmete kasutamisel?

Andmete päritolu ja kogumise viisi põhjal saab eristada esmaseid ja teiseseid andmeid. **Esmased ehk primaarsed isikuandmed** kogutakse vahetult inimeselt, **teisesed ehk sekundaarsed isikuandmed** on algul muul eesmärgil kogutud ja neid ei saada inimeselt endalt, vaid andmebaasidest, arhiividest või mujalt.

Esmaste andmete töötlemine teadusuuringus on üldjuhul lihtsam ja sirgjoonelisem, kuna õiguslik suhe tekib vaid andmekoguja ja andmesubjekti vahel, õiguslikuks aluseks on nõusolek ning kogu vastutus isikuandmete töötlemise eest lasub vastutaval töötlejal. Teiseseid isikuandmeid töödeldakse aga sageli nõusolekuta ning lisaks andmesubjektile peab arvestama ka andmete valdaja kohustuste ja huvidega. Seega on teiseste isikuandmete töötlemine üldiselt keerulisem, kuna kehtib mitu erandit.

2.8.1. Teisene kasutus võib olla kooskõlas esialgse eesmärgiga

Kui olemasolevate isikuandmete plaanitav uus kasutus on kooskõlas esialgse eesmärgiga, milleks andmed koguti, ei vaja see üldjuhul eraldi õiguslikku alust. Seega tuleb teiseste andmete kasutamisel hinnata, kas isikuandmete töötlemise esialgne ja uus eesmärk on omavahel kooskõlas. Teadustöö puhul eeldatakse üldmääruse artikli 5 lg 1 p b ja põhjenduse 50 kohaselt küll alati kooskõla algse eesmärgiga, kuid see ei tähenda, et igasuguste varem kogutud isikuandmete töötlemine teadusuuringus on automaatselt lubatud. Vastutav töötleja peab arvestama ka teiste andmekaitsepõhimõtetega ning veenduma nende põhjal teiseste andmete kasutamise lubatavuses.

Kuigi ei ole üht kindlat põhimõtet, mille põhjal algse ja uue eesmärgi kooskõla hinnata, eeldatakse, et kooskõla on suurem, kui mõlema eesmärgi saavutamiseks töötleb andmeid sama vastutav töötleja. Kooskõla on väiksem või puudub üldse, kui isikuandmed antakse üle uuele vastutavale töötlejale, kui algne ja uus kasutus erinevad märgatavalt, kui töödeldakse eriliiki isikuandmeid või kui töötlemisega kaasneb suurem oht inimeste õigustele ja vabadustele.

Kui uus eesmärk ei ole algsega kooskõlas, on andmete töötlemiseks vaja uut õiguslikku alust (vt ka p-d 1.5.3 ja 2.8.4).

2.8.2. Teabe andmine andmesubjektile teiseste andmete kogumisel

Kui esmaste isikuandmete puhul antakse kogu oluline teave andmesubjektile vahetult kas kogumise ajal või enne seda, siis teiseste uuringute puhul, kui isikuandmeid ei koguta otse andmesubjektilt, kehtivad teavitamiskohustuse suhtes mõningad erandid (vt üldmääruse artikkel 14). Näiteks ei ole teavitamiskohustust, kui teabe esitamine osutub võimatuks või eeldab ebaproportsionaalseid jõupingutusi (andmed on kogutud kaua aega tagasi või andmesubjektide hulk on väga suur). Siiski tuleb teave andmesubjekti õiguste ja huvide kaitsmiseks avalikustada näiteks teadusasutuse või -projekti veebilehel. Sellisel juhul ei ole vastutaval töötlejal kohustust andmesubjektiga ühendust võtta, kuna eeldada võib, et andmesubjekt leiab ise vajaliku teabe üles.

2.8.3. Teiseste andmete valdajad

Isikuandmete teisest kasutust soositakse näiteks üldmääruse artikli 5 lg 1 p-s b nimetatud eesmärgi piirangu, IKS-i § 6 lg-te 1 ja 3 ja seletuskirja põhjenduste kohaselt. Selle keerukust suurendab aga asjaolu, et arvestama peab andmeid valdava asutuse kohustustega andmesubjektide suhtes. Andmekaitseõigusest ei tulene kohustust anda teadlastele teiseseid isikuandmeid, kuid võttes arvesse teaduse tegemise vabadust ja Euroopa Liidu pühendumust avatud teadusele, infovabadust ja avalike asutuste kohustust anda teavet, edastavad avalikud asutused – sealhulgas avalike andmekogude ja registrite pidajad – üldjuhul teadlastele nende küsitud teabe, kui täidetud on kõik selleks ettenähtud nõuded. Seda toetab ka IKS-i seletuskiri, kus § 6 lg 3 nõuete hindamise kohta on öeldud: „Tavapäraste isikuandmetega tehtavad uuringud ei vaja Andmekaitse Inspektsiooni või eetikakomitee luba. Kui teadustöö vms tegija tingimused täidab, tuleb talle võimaldada juurdepääs teabele, näiteks andmekogudele.“

Avalike andmekogudega on olukord lihtsam. Palju rohkem raskusi tekib erasektoriga, kelle valduses olevat teisest teavet võib kaitsta ärisaladus. Seega jääb alati võimalus, et isegi kui teadlane on hoolikalt hinnanud isikuandmete töötlemise vajadust, selle suhtes esinevat avalikku huvi ja andmesubjektide õiguste riivete proportsionaalsust, keeldub andmete valdaja ikkagi teiseseid andmeid väljastamast.

2.8.4. Teiseseks kasutuseks tuleb leida sobiv õiguslik alus

Et esmased andmed kogunud vastutav töötleja võiks need edastada teadlasele või teadusasutusele ning see teadlane või asutus saaks need teiseseks töötlemiseks vastu võtta, peab mõlemal poolel olema õiguslik alus.

- **Avalikes huvides ülesanne teisese kasutuse õigusliku alusena**

Avalikes huvides ülesande kasutamine õigusliku alusena eeldab eelkõige teadustööga seotud avaliku huvi hindamist. IKS-i §-ga 6 on lubatud isikuandmeid teadusuuringutes ilma nõusolekuta töödelda, kuid sellele on seatud lisanõuded: pseudonüümimine (lg 1) või erandkorras isikustatud andmete kasutamine (lg 3, vt ka alaptk 2.4).

Samuti peab teadlane tõendama avalikku huvi. Selleks puudub selgelt kokku lepitud vorm või standard, kuid kuna avalikku huvi põhjendatakse ka teadustöö rahastajale või eetikakomiteele, võiks eetikakomitee kooskõlastusest üldjuhul piisata, et veenda andmete valdajat avaliku huvi olemasolus. Siiski pole välistatud, et andmete valdaja soovib ka muul viisil avalikes huvides ülesande õigusliku aluse tõestamist.

- **Nõusolek teisese kasutuse õigusliku alusena**

Nõusolek ei pruugi teisese kasutuse puhul otstarbekas olla, sest andmeid küsival teadlasel on keeruline, kui mitte võimatu saada seda andmesubjektidelt, kellega tal puudub kontakt. Siiski saaks nõusolekut küsida andmete valdaja, kui see on mõistlikult võimalik: ta võib esitada ühekordse päringu või kasutada muud lahendust, näiteks nõusolekuteenust. Nõusolek annaks mõlemale vastutavale töötlejale kindluse, et andmete väljastamine konkreetse teadusuuringu jaoks on seaduslik. Ühtlasi tagab see uuringualuse suurema kontrolli oma andmete üle.

Isikuandmete teiseseks kasutamiseks teadusuuringutes on aga võimalik küsida nõusolek juba esmaste andmete kogumisel. Sel juhul on andmeid valdaval asutusel kindlus, et tal on õigus anda isikuandmeid teadlastele või teadusasutustele, keda ta usaldab. Samas tuleb arvestada inimestele esialgses nõusolekus lubatut. Kui näiteks esmaste andmete kogumisel anti lubadus, et andmeid säilitatakse viis aastat pärast projekti lõppu ja seejärel need hävitatakse, siis peab ka andmete teisene kasutus selle tähtaja sisse mahtuma (vt ka alaptk 2.3).

2.8.5. Eriliiki isikuandmete jaoks on nõutav eetikakomitee kooskõlastus

Kui teiseseks kasutuseks vajatakse eriliiki isikuandmeid ja nende töötlemine ei toimu nõusoleku alusel, on IKS-i § 6 lg 4 kohaselt vaja eetikakomitee kooskõlastust. Kui andmeid väljastatakse tervise infosüsteemist või geenivaramust, tuleb see kooskõlastada muude seaduste alusel. Eetikakomitee kooskõlastus on vaid lisakaitsemeede, mis ei anna teiseseks töötlemiseks õiguslikku alust. Õiguslik alus saaks nõusolekuta uuringu puhul olla avalikes huvides ülesanne (vt ka alaptk 2.13).

2.8.6. Teiseste andmete edastamiseks võib olla vaja sõlmida leping

Isikuandmete saamiseks on võimalik sõlmida andmevaldajaga leping, milles lepitakse kokku isikuandmete töötlemise tingimused, eesmärgid ja tähtajad. See aitab andmevaldajal kontrollida, et välja

antud andmeid töödeldakse nõuetekohaselt, ja seada muu hulgas tingimused andmete hävitamise või pikaaegse säilitamise kohta.

Isikuandmed saanud teadusasutus on nende edasisel töötlemisel vastutav töötleja. Seega vastutavad nii teadusasutus kui ka teadlane asutuse esindajana isikuandmete teisese kasutamise korral kõigi üldmääruse nõuete täitmise eest isegi juhul, kui eraldi lepingut ei ole sõlmitud. Vaid juhul, kui andmed anonüümitakse enne väljastamist ja neid ei saa enam ühelgi viisil andmeid väljastava asutuse valduses olevate isikustatud andmetega seostada, ei kaasne teadlastele ja teadusasutustele andmekaitsealast vastutust.

2.8.7. Avalikustatud isikuandmete teisene kasutamine

Andmekaitsepõhimõtted kehtivad ka meedias avalikustatud isikuandmete suhtes. Seega tuleb nende teisese kasutamise korral mõelda, milline on sobiv õiguslik alus nende töötlemiseks või kuidas anda inimestele plaanitava teadustöö kohta teavet. Näiteks võib sotsiaalmeedia keskkondadest tuhandete inimeste andmete kogumisel kõigilt nõusoleku küsimine või kõigile teabe edastamine olla erakordselt keeruline. Erandite kasutamisel ja võimalike alternatiivide otsimisel tasub meeles pidada, et eesmärk on vältida inimeste huvide ja õiguste kahjustamist, austada inimeste õigust otsustada oma andmete üle ja tagada seejuures teadustöö läbipaistvus ja usaldusväärsus.

Keskkonnad, kust avalikustatud isikuandmeid kogutakse, on enamasti oma kasutustingimustes täpsustanud, kuidas ja milleks on lubatud andmeid kasutada. Mõni keskkond on loonud eraldi rakendusliidesed, mille kaudu saab automatiseeritult andmeid koguda. Kõigil sellistel juhtudel tuleb järgida ka keskkonna valdaja nõudeid ja tingimusi, et andmete kogumine oleks õiguspärane. Samas võib mõni ettevõte seada ebamõistlikke piiranguid nende valduses olevate andmete töötlemisele teadustöö eesmärgil. Nagu selle alapeatüki sissejuhatuses mainitud, ei ole erasektori valduses olevate teadusliku väärtusega isikuandmete puhul alati selge, kas kaalukamad on ettevõtete erahuvid või teaduse huvid.

Loe lisaks

- Internetiuurijate Assotsiatsiooni (AoIR) suunis „Ethical Guidelines 3.0“ (2019: 14)
- AoIR-i varasemad internetiuuringute eetika juhendmaterjalid

2.9. Kuidas arvestada teadustöös inimeste õigustega oma andmete üle?

Üldmääruse III peatükis on nimetatud andmesubjekti õigused, mis on tal alati olemas sõltumata isikuandmete töötlemise eesmärgist või õiguslikust alusest. Seega võib uuringus osaleja esitada teadlasele päringu enda andmete töötlemise kohta isegi juhul, kui uuringus kasutatakse avalikust registrist saadud pseudonüümitud andmeid. Segaduste vältimiseks on hea, kui teadusrühmas on aegsasti kokku lepitud, kes on uuringuga seotud isikuandmete eest vastutav töötaja. Temal tuleb ka päringule vastata.

Allpool on loetletud andmesubjekti õigused ja neid lühidalt selgitatud.

2.9.1. Õigus saada teavet isikuandmete töötlemise kohta

Üldmääruse artiklites 12, 13 ja 14 sätestatakse üldine teabe saamise õigus, mille tõttu on vastutaval töötlejal kohustus koostada ja avaldada andmekaitsetingimused ning teavitada neist andmesubjekti. Kui

teadlasel on võimatu või ebamõistlikult keeruline inimestega ühendust võtta, piisab teabe avalikult kättesaadavaks tegemisest. Teabe esitamine toetab läbipaistvus- ja õigluspõhimõtet.

Teadusuuringute puhul on peamine teabevahend uuringus osaleja nõusoleku küsimisel talle antav infomaterjal. Siiski tuleb arvestada, et andmesubjektil on õigus enda isikuandmete töötlemise kohta igal ajal teavet küsida, mistõttu ei pruugi infomaterjali edastamine või vastutava töötleja andmekaitsetingimustele viitamine olla piisav ning tagatud peab olema uuritava võimalus teadusuuringu tegijaga ühendust võtta.

Inimesele jääb õigus saada teavet oma andmete töötlemise kohta ka siis, kui isikuandmeid ei töödelda tema nõusolekul, vaid muul õiguslikul alusel.

2.9.2. Õigus andmetega tutvuda

Üldmääruse artiklis 15 antakse andmesubjektile õigus tutvuda tema kohta kogutavate andmete, nende vastuvõtjate, kolmandatesse riikidesse edastamise, allikate (kui andmed ei pärine andmesubjektilt) ning teabe põhjal tehtavate automatiseeritud otsuste kohta. Samuti võib ta küsida üldisemat teavet, mis puudutab uuringu eesmärkide ja säilitamise aega.

Oma andmetega tutvumiseks peab andmesubjekt esitama sellekohase taotluse vastutavale töötlejale, kellel on enne andmete väljastamist õigus taotleja tuvastada, et veenduda, kas see on sama inimene, kelle andmeid küsitakse. Kui taotlus on saadetud e-kirjaga, tuleb küsida digitaalselt allkirjastatud taotlust.

Kui isik on tuvastatud, on tal Tartu Ülikoolis kaks võimalust oma isikuandmete kohta teavet saada: ta võib tulla nendega tutvuma kohapeale või saada koopia oma andmetest. Ainus erand, mille puhul kumbagi võimalust kasutada ei saa, kehtib juhul, kui andmesubjekti andmeid sisaldava baasi või keskkonna näitamine või koopia esitamine tekitaks kellelegi kahju – näiteks on näha ka teiste isikute andmed. Sel juhul andmetega kohapeal tutvuda ei saa ja koopiat ei väljastata, vaid taotlejale antakse üksnes kirjeldav tekst. Sealjuurest tuleb kindlasti selgitada, miks ta ei saa kohapeale tulla või miks talle koopiat ei anta.

IKS-i § 6 lg 6 alusel võib vastutav töötleja andmetega tutvumise õigust piirata, kui selle järgimine muudab teadusuuringu eesmärgi täitmise võimatuks või takistab seda oluliselt.

2.9.3. Õigus andmete parandamisele

Üldmääruse artikli 16 kohaselt on andmesubjektil õigus nõuda ebatäpsete andmete parandamist või mittetäielike andmete täiendamist. See õigus on seotud andmete kvaliteedi põhimõttega ja tagab, et inimese kohta tehtavad otsused ei põhineks valedel või poolikul teabel.

Vastutav töötleja on kohustatud alati teavet andmesubjekti taotluse järgi parandama või täiendama, välja arvatud juhul, kui töötleja hinnangul on andmed täielikud või õiged. Sel juhul tuleb oma otsust ka andmesubjektile põhjendada.

IKS-i § 6 lg 6 annab vastutavale töötlejale võimaluse andmete parandamise õigust piirata, kui selle järgimine muudab teadusuuringu eesmärgi täitmise võimatuks või takistab seda oluliselt.

Näide

Mõni päev pärast intervjuud pöördub intervjueeritu uurija poole palvega täpsustada oma vastust ühele küsimusele. Kui teadlasel on võimalik seda teha ja see on uuringu selles etapis mõeldav, tuleks see palve

täita. Kui aga sama inimene pöördub korduvalt pikema aja vältel aina uue sooviga üht või teist vastust täpsustada, hakkab see juba teadustööd takistama. Seda, kust täpselt läheb piir põhjendamatu takistamise ja põhjendatud täpsustuse vahel, on keeruline öelda. Andmesubjektile tuleb igal juhul selgitada põhjuseid, miks ta ei saa enam mingil hetkel oma vastuseid täpsustada.

2.9.4. Õigus andmete kustutamisele

Üldmääruse artiklis 17 on sätestatud õigus andmete kustutamisele – see on tuntud ka kui *õigus olla unustatud*. Andmete kustutamine on üks keerulisemaid õigusi. Seda tuleb teha, kui kehtib üks järgmistest üldmääruses nimetatud asjaoludest:

- kui andmete töötlemise eesmärk on täidetud;
- kui andmete töötlemine on ebaseaduslik;
- kui isik võtab nõusoleku tagasi ja puudub muu õiguslik alus;
- kui andmesubjekt on vaidlustanud enda andmete töötlemise ja edasine töötlemine ei ole põhjendatud;
- kui see on vajalik juriidilise kohustuse täitmiseks;
- kui andmed puudutavad infoühiskonna teenuse kasutamist ajal, mil andmesubjekt oli alaealine.

Siiski on andmete kustutamise õiguse puhul mitu erandit, mil vastutaval töötlejal on õigus jätkata isikuandmete töötlemist, isegi kui andmesubjekt esitab taotluse nende kustutamiseks. Sellised on näiteks juhud, kui töötlemine on vajalik avalikes huvides toimuva teadusuuringu eesmärgil, andmete kustutamine muudaks teadusuuringu eesmärkide saavutamise võimatuks või häiriks seda suurel määral. Andmete kustutamine teadusuuringutes on üldse pigem erandlik.

Isikuandmeid saab pikemat aega säilitada siis, kui need anonüümida või teha otsus hoida need alles arhiveerimise eesmärgil (vt alaptk 4.1). Isikuandmete kogumise ajal tuleb aga anda inimesele teada, kuidas ja kui kaua on plaanis neid säilitada.

2.9.5. Õigus andmete töötlemise piiramisele

Üldmääruse artikli 18 kohaselt on andmesubjektil õigus piirata isikuandmete töötlemist neljal juhul, millest teadusuuringute kontekstis on asjakohased kolm:

- kui andmete õigsus on vaidlustatud, saab töötlemist piirata ajaks, mil andmete õigsust kontrollitakse;
- kui andmete töötlemine vaidlustatud, saab töötlemist piirata ajaks, mil kontrollitakse, kas vastutava töötleja huvid kaaluvad üles andmesubjekti huvid;
- kui isikuandmete töötlemine on ebaseaduslik ehk selleks puudub õiguslik alus, võib andmete kustutamise asemel nõuda töötlemise piiramist.

Üldmääruses sätestatakse üksikud erandid, mille kohaselt on vastutaval töötlejal siiski lubatud töötlemispiiranguga andmeid töödelda: eelkõige andmesubjekti nõusolekul, õigusnõuete koostamise eesmärgil, teiste isikute õiguste kaitseks või olulise avaliku huvi korral.

IKS-i § 6 lg 6 kohaselt ei pea vastutav töötleja isikuandmete töötlemise piiramise õigust täiel määral järgima, kui see muudab teadusuuringu eesmärgi täitmise võimatuks või takistab seda oluliselt. Töötlemise piiramine teadusuuringute puhul on siiski väga erandlik ja vähetõenäoline. Peamiselt võidakse seda teha siis, kui inimene võtab tagasi nõusoleku oma andmete töötlemiseks, kuid otsustab kustutamise asemel nõuda andmete töötlemise piiramist. Sellisel juhul võib andmeid säilitada, kuid

nende kasutamine peab olema piiratud. Ent kuna andmete kustutamine puudutabki enamasti juhtumeid, mil töötlemiseks puudub õiguslik alus, oleks andmete edasine töötlemine niikuinii keelatud.

2.9.6. Andmete ülekandmise õigus

Üldmääruse artikliga 20 antakse andmesubjektile võimalus viia oma andmeid ühe vastutava töötleja juurest teise juurde. Selle toimingu suhtes kehtib paar piirangut:

- üle saab kanda üksnes andmeid, mille töötlemise õiguslikuks aluseks on nõusolek või leping;
- nõutud andmete töötlus peab olema automatiseeritud ja ülekandmine ühelt töötlejalt teisele tehniliselt teostatav;
- ülekantavad andmed peavad olema struktureeritud, üldkasutatavas vormingus ja masinloetaval kujul;
- ülekandmist saab nõuda vaid nende andmete suhtes, mille andmesubjekt on ise vastutavale töötlejale andnud.

Kuna enamik teadusuuringuid põhineb nõusolekul ja automatiseeritud andmetöötlusel, on inimesel põhimõtteliselt alati võimalik nõuda enda andmete ülekandmist.

Näide

Inimene kolib elama teise Euroopa Liidu liikmesriiki ja kavatseb seal veeta ülejäänud osa oma elust. Kuna ta on aastaid tagasi andnud geenivaramusse geeniproovi, soovib ta kõigi endaga seotud andmete ülekandmist uue elukohariigi analoogsesse geenipanka, kust tema uuel arstil oleks lihtsam tema kohta teavet saada. Ta saab üle kanda vaid andmeid, mille ta on ise geenivaramule andnud, st üksnes oma tervisekirjelduse, kuid mitte geeniandmeid, mille geenivaramu on lisaanalüüside põhjal koostanud.

2.9.7. Õigus esitada vastuväiteid

Üldmääruse artiklis 21 on sätestatud andmesubjekti õigus vaidlustada oma andmete töötlemine õigustatud huvi või avalikes huvides ülesande alusel, olenemata sellest, kui põhjalikult on neid õiguslikke aluseid põhjendatud. Kui vaie on edukas, tühistatakse õiguslik alus, töötlemine muutub ebaseaduslikuks ja tekib õigus nõuda andmete kustutamist või piiramist. Vastuväite hindamise ajaks võib nõuda ka andmete töötlemise piiramist.

IKS-i § 6 lg 6 alusel võib vastutav töötleja vastuväite esitamise õigust piirata, kui selle järgimine muudab teadusuuringu eesmärgi täitmise võimatuks või takistab seda oluliselt. Kuna õigusliku aluse vaidlustamine takistab paratamatult teadusuuringu eesmärkide saavutamist, ei ole päris selge, mida vastutav töötleja sellise taotluse korral tegema peaks. Arvestama peab siiski võimalusega, et kui taotlust arvesse ei võeta, võib andmesubjekt pöördada oma õiguste kaitseks Andmekaitse Inspektsiooni poole või kohtusse.

2.9.8. Õigus olla kaitstud automatiseeritud töötlemisel põhinevate otsuste eest

Üldmääruse artikliga 22 ei keelata isikuandmete automaattöötlust täielikult ära. Lubamatu on aga teha pelgalt automatiseeritud töötlusel, sealhulgas **profiilianalüüsil** (artikli 4 lg 4) põhinevat otsust, mis avaldab andmesubjektile märkimisväärset mõju või toob kaasa õiguslikke tagajärgi.

Siiski esineb siin kolm erandit. Automatiseeritud töötlemisel põhineva otsuse tegemine ei ole keelatud, kui see

- on vajalik lepingu sõlmimiseks või täitmiseks;

- on seadusega lubatud;
- põhineb andmesubjekti eraldi antaval nõusolekul konkreetselt automaattöödeldud otsuste tegemise kohta. Selline nõusolek peab olema muudest nõusolekuvormi tingimustest eristatud.

Teadusuuringute puhul ei ole selle õiguse suhtes tehtud ühtki erandit. Seega on automatiseeritud isikuandmete töötlemine, sh profiilianalüüs, keelatud, kui sellise töötlemise käigus või tulemusena tehakse kohta otsuseid, millel on uuritavatele märkimisväärne mõju või mis toovad kaasa õiguslikke tagajärgi (näiteks piiratakse nende põhjal ligipääsu avalikele teenustele). Enamasti teadustöös isikute kohta selliseid otsuseid ei langetata, ehkki mõnda tüüpi rakendusuuringutes on teoreetiliselt võimalik luua ja arendada selliseid automatiseeritud töötlemise meetodeid, mida saab hiljem kasutada isikute kohta otsuste tegemisel.

2.10. Mida pidada silmas haavatavate isikute andmete töötlemisel?

Hea teadustava sõnastiku kohaselt on isikud või rühmad haavatavad, kui nad ei suuda või ei saa oma tahet vabalt väljendada (piiratud autonoomia) või kui nad on oma tervise, töö, hariduse või muude tunnuste tõttu vastuvõtlikud kahjudele.

Haavatavusega arvestamine on kooskõlas üldiste teaduseetika põhimõtetega – eelkõige inimese autonoomia austamise, kahju tegemata jätmise ja hea tegemisega. Isikuandmete õiglase töötlemise põhimõtted (vt alaptk 2.6) eeldavad muu hulgas haavatavuse hindamist: arvestama peab andmesubjekti ootustega, tema ekspluateerimine ja diskrimineerimine on keelatud, töötlemise eesmärk ja viis peavad olema eetilised.

2.10.1. Haavatavad isikud ja rühmad

Haavatavaks peetakse sageli lapsi, eakaid, rasedaid, looteid, kinnipeetavaid ja vange, puudega inimesi, rahvusvähemusi, vaeseid, kodutuid, kirjaoskamatuid, töötuid ja vägivallaohvreid. See nimekiri ei ole mõistagi ammendav ega universaalne.

Andmekaitse ei erista andmesubjekte mingite lisatunnuste alusel, vaid annab kõigile võrdse ja ühetaolise õiguse oma isikuandmete kaitsele. Üldmääruse ainus erand on lapsed, kelle isikuandmete kaitset rõhutatakse eraldi. See aga ei tähenda, nagu ei oleks haavatavus andmekaitsevaldkonnas oluline, eriti kui hinnatakse andmetöötluse mõju inimeste õigustele ja vabadustele (eelkõige seoses diskrimineerimisega) või teadustöö eetilisust.

2.10.2. Haavatava isiku nõusolek ei pruugi olla vabatahtlik

Kui haavatavus seisneb inimese piiratud võimaluses oma tahet vabalt väljendada, on oluline kindlaks teha, kas ja kuivõrd võib see mõjutada tema antava nõusoleku vabatahtlikkust. Samuti tuleb arvestada inimese võimet teabest aru saada ja mõista oma otsuse tagajärgi.

Teabest arusaamise lihtsustamiseks võib kasutada lihtsamat keelt või selgitavaid illustratsioone. Kuigi Eestis ei ole üldist kohustust küsida haavatavate isikute uuringusse kaasamisel eetikakomitee kooskõlastust, on hea tava seda siiski teha, et tagada nende huvide ja õiguste parem kaitse. Eetikakomitee kooskõlastus annab lisagarantii, et inimeste haavatavust on uuringus piisavalt arvestatud.

2.10.3. Haavatavate isikute andmete töötlemine võib ohustada nende õigusi ja huve

Isikuandmete töötlemisega võib kaasneda haavatavate isikute tavapärasest suurem diskrimineerimise või stigmatiseerimise oht. See võib kaasa tuua vajaduse koostada andmekaitsealane mõjuhinnang, milles tuleks põhjalikult hinnata võimalikke tagajärgi uuringusse kaasatutele ja kavandada lisameetmeid riskide maandamiseks (vt ka alaptk 2.14).

2.11. Mida pidada silmas eriliiki isikuandmete töötlemisel?

Eriliiki isikuandmete töötlemine on keelatud, välja arvatud juhul, kui töötlemiseks on õiguslik alus ja lisaks kehtib üks üldmääruse artikli 9 lg-s 2 nimetatud asjaolu. Teadustööd puudutavad neist kõige otsesemalt kaks: kui inimene on andnud eriliiki isikuandmete töötlemiseks nõusoleku või kui töötlemine on vajalik avalikes huvides toimuva teadusuuringu eesmärgil. Viimasel juhul peavad aga olema kasutusele võetud lisakaitsemeetmed, töötlemine peab olema seaduslik ja austada tuleb inimeste õigusi. Eestis peab eriliiki isikuandmete töötlemisel järgima ka IKS-i § 6.

2.11.1. Eriliiki isikuandmete nõusolekuta töötlemiseks peab olema eetikakomitee kooskõlastus

Eetikakomitee kooskõlastuse kohustus on sätestatud isikuandmete kaitse seaduse § 6 lg-s 4 ja see kehtib juhul, kui teadusuuringus töödeldakse eriliiki isikuandmeid ilma andmesubjekti nõusolekuta. Seda kohustust võib vaadata kui lisakaitsemeedet üldmääruse artikli 9 lõike 2 punkti j tähenduses. Eetikakomiteele esitatavas kooskõlastustaotluses tuleb andmesubjekti õiguste ja isikuandmete kaitsmiseks plaanitavaid meetmeid kirjeldada.

2.11.2. Eriliiki isikuandmete töötlemine vajab lisakaitsemeetmeid

Kuna eriliiki isikuandmed on väga tundlik teave, kaasneb sellega risk kahjustada inimeste huve ja õigusi. Seepärast vajavad eriliiki isikuandmed rohkem kaitset:

- eelistada tuleb töötlemist pseudonüümitud kujul või kasutada muid kaitset pakkuvaid lahendusi, näiteks krüpteerimist;
- enne töötlema asumist tasub hinnata, kas tuleb teha ka andmekaitsealane mõjuhinnang (vt p 2.14.3), eriti kui uuritavate hulka kuuluvad haavatavad inimesed.

2.11.3. Eriliiki isikuandmete mõiste kohaldamine on kohati keeruline

Vahel on eriliiki ja tavaliste andmete vahele raske piiri tõmmata. Näiteks ei ole täit kindlust selles, millal uuritakse vaimset tervist ja millal meelsust või hoiakuid.

Abiks võib olla eesmärgipõhine lähenemine. Kui inimese hoiakute ja enesetunde kohta kogutakse andmeid selleks, et teha järeldusi näiteks tema stressitaseme või -taluvuse kohta, on tegemist vaimse tervise uurimisega. Kui aga neid andmeid küsitakse selleks, et uurida rahulolu töö või mõne teenusega, ei puuduta see vaimset tervist, vaid muid näitajaid.

2.12. Kui täpselt tuleks sõnastada teadusuuringu eesmärk?

Ehkki teadusuuringu eesmärk peaks olema sõnastatud võimalikult konkreetselt, ei pruugi see andmete kogumise hetkel lõplikult teada olla ja lubatud on mõningane paindlikkus. Seetõttu võimaldab üldmäärus sõnastada teadusuuringu eesmärgi laiemalt, näiteks distsipliini või valdkonna täpsusega.

Teadusuuringu eesmärki tuleb eristada muust teadustööd toetava tegevuse eesmärkidest. Kui näiteks nõusolekuvormi kaudu on teadlasele teada inimeste kontaktandmed, ei ole tal lubatud nende kontaktandmete alusel neid uude teadusprojekti kutsuda, kui selleks puudub eelnev nõusolek. Samuti ei tohi samu andmeid kasutada mõnes järgmises projektis, kui seda ei ole uuringualustele eraldi öeldud. Üldmääruse tõlgenduse kohaselt on andmete teisene kasutus teadusuuringu eesmärgil küll lubatud, kuid siis tuleb andmesubjekti sellest teavitada (vt alaptk 2.8).

Kui uuringul on mitu eesmärki, tuleb juhul, kui töötlemise õiguslikuks aluseks on nõusolek, küsida seda igaks eesmärgiks eraldi.

2.13. Millal on tarvis eetikakomitee kooskõlastust?

Kooskõlastust võib käsitleda lisakaitsemeetmena, mis aitab tagada, et teadustöö tegemisel on käitutud eetiliselt. Mõnel juhul võib eetikakomitee kooskõlastus olla **seadusest tulenev kohustus**, teinekord võib see olla vajalik **rahastaja või kirjastuse nõuete** täitmiseks ja vahel võib eetikakomitee poole pöörduda ka **eetilistel kaalutlustel**.

Enamasti sõltub eetikakomiteelt kooskõlastuse küsimine sellest, kas teadlane soovib teha inimuuringut või mitte. Inimuuringute käigus töödeldakse isikuandmeid ning uuritakse osaleja füüsilist või vaimset tervist. Osa inimuuringuid on Eestis eraldi seadusega reguleeritud, näiteks ravimite ja meditsiiniseadmete kliinilised uuringud ja inimgeeniuuringud.

Loe lisaks

- TÜ inimuuringute eetikakomitee veebileht
- Euroopa Andmekaitseinspektori esialgne arvamus andmekaitse ja teadusuuringute kohta (lk 12)
- Eesti bioeetika ja inimuuringute nõukogu juhendid taotluse esitamiseks

2.13.1. Seadusest tulenev kohustus

IKS-is nähakse ette, et eetikakomitee hindab lisaks uuringueetilistele aspektidele ka andmekaitsenorme. Eestis on eetikakomitee kooskõlastus seadusega kohustuslik, kui

- töödeldakse isiku nõusolekuta eriliiki isikuandmeid, näiteks tervise- või biomeetrilisi andmeid (IKS-i § 6 lg 4);
- andmeid töötleb geenivaramu (inimgeeniuuringute seaduse § 29), sealhulgas juhud, kui geenidoonori andmed depseudonüümitakse (inimgeeniuuringute seaduse § 24);
  - isikuandmed väljastatakse tervise infosüsteemist (tervishoiuteenuste korraldamise seaduse § 59^4);
- tehakse ravimi kliinilist uuringut (ravimiseaduse § 93);
- tehakse meditsiiniseadme kliinilist uuringut (meditsiiniseadme seaduse § 21^3).

Mitmel juhul on seadusega sätestatud, millise eetikakomitee poole tuleb pöörduda. Eesti geenivaramu ning tervise infosüsteemi andmete väljastamisega seotud uuringuid kooskõlastab Eesti Bioeetika ja Inimuuringute Nõukogu, ravimi kliinilisi uuringuid Ravimiameti juurde loodud ravimiuuringute eetikakomitee, meditsiiniseadme kliinilisi uuringuid Tartu Ülikooli inimuuringute eetikakomitee ning Tervise Arengu Instituudi inimuuringute eetikakomitee. Mõnikord tuleb tervise infosüsteemi ja muudest allikatest pärit andmete ühendamiseks küsida kooskõlastus mitmest eetikakomiteest.

Vahel on aga täpsustamata, milline peaks IKS-i § 6 lg 4 kohane eetikakomitee olema. Sel puhul sobib kooskõlastuse saamiseks iga omas valdkonnas tunnustatud eetikakomitee.

2.13.2. Rahastajate ja kirjastajate nõuded

Kooskõlastust võib nõuda ka projekti rahastaja või kirjastus, kus soovitakse teadustöö avaldada. Kui rahvusvahelise projekti juhtpartner on näiteks otsustanud, et eri uuringute jaoks küsitakse riiklike eetikakomiteede kooskõlastus, peavad ka Eesti teadlased selle muretsema.

Näide
Meditsiiniteadlane tegi uuringu, mille jaoks ta ei pidanud tarvilikuks eetikakomitee kooskõlastust hankida, sest tegu ei olnud eriliiki andmetega. Pärast uuringu valmimist soovis ta avaldada selleteemalise artikli rahvusvahelises ajakirjas. Kirjastaja nõudis teadlaselt eetikakomitee kooskõlastust. Kuna aga eetikakomitee tagantjärele kooskõlastust ei anna, jäigi artikkel rahvusvahelises ajakirjas avaldamata. Seega – ehkki kooskõlastus ei ole alati kohustuslik, võib selle puudumine vähendada teadlase publitseerimisvõimalusi.

2.13.3. Eetilised kaalutlused

Teadlane võib küsida eetikakomitee kooskõlastust ka eetilistel kaalutlustel, kuna see aitab paremini tagada, et plaanitav uuring inimesi ei kahjusta. Kooskõlastus on üldjuhul vajalik juhul, kui teadusuuring korraldatakse tavapärasest väga erineva meetodi abil (näiteks kui inimesi eksitatakse või petetakse), kui uuritakse haavatavaid isikuid või kui uuringuga seondub tavapärasest suurem risk.

Lisaks võib teadlane alati vabatahtlikult eetikakomitee poole pöörduda.

Loe lisaks
- TÜ inimuuringute eetikakomitee juhendid ja nõuded
- Euroopa Andmekaitseinspektori esialgne arvamus andmekaitse ja teadusuuringute kohta (lk 12)

2.14. Kuidas hinnata isikuandmete töötlemisega kaasnevaid riske?

Üks keskseid teaduseetilisi põhimõtteid on, et teadustööst peaks sündima võimalikult palju kasu ja võimalikult vähe kahju. Mõnikord on kahju vältimatu, kuid enamjaolt on seda võimalik põhjaliku riskide hindamise ja maandamisega vähendada.

2.14.1. Riskihindamise üldmeetod

Mõnikord nõuavad teadusuuringute rahastajad, et teadlased hindaks teadustööga seotud eetilisi riske ja kirjeldaks, kuidas neid riske maandada. Oma teadusuuringut kavandades või sellele granti taotledes võib ka teadlasel endal tekkida vajadus oma teadustööga seotud riske hinnata.

Üldjuhul hinnatakse riske mitmes etapis.

- **Riskide tuvastamise** etapis loetletakse kõik võimalikud riskid. Selleks ei ole üht ainuõiget viisi. Mõnikord delegeeritakse see ülesanne ekspertidele või projekti juhtpartnerile, kuid seda võivad teha ka teadustööga seotud teadlased. Kuna tuvastada tuleks ka harva esinevaid ohte, on rohkemate inimeste kaasamine alati kasulikum.

Ka siis, kui riski ei tuvastata, näitab see välishindajatele (Euroopa Komisjon, Eesti Teadusagentuur, Andmekaitse Inspektsioon, eetikakomitee), et võimalikele ohtudele on mõeldud, neid ei esine ja lisameetmed pole vajalikud.

- **Riskide analüüsimise** etapis antakse igale tuvastatud ohule hinnang selle tõenäosuse ja võimaliku mõju alusel. Kõige lihtsam ja enamasti piisav on lahendus, kus tõenäosust ja mõju hinnatakse viiepallisel skaalal („väga väike“, „väike“, „keskmine“, „suur“ ja „väga suur“) ja riski kolme värvuse alusel (roheline, kollane ja punane). Nende põhjal koostatakse riskimaatriks, mille põhjal tõenäosuse ja mõju hinnangud summeeritakse. Allolevas tabelis tähistab suurt riski punane värvus, keskmist riski kollane ja väikest roheline.

  Tabel. Riskide jagunemine tõenäosuse ja mõju tugevuse järgi

TÕENÄOSUS	MÕJU				
	Väga väike	Väike	Keskmine	Suur	Väga suur
Väga väike	0	1	2	3	4
Väike	1	2	3	4	5
Keskmine	2	3	4	5	6
Suur	3	4	5	6	7
Väga suur	4	5	6	7	8

  Riskide hindamiseks leidub ka muid meetodeid ning mõju, tõenäosuse ja riski skaalad võivad neis erineda.

- **Riskide hindamise** etapis tuleb otsustada, millised riskid on väikesed ja millised on keskmisest suuremad, nii et neid tuleb maandada. Selleks tuleb välja pakkuda meetmed, mis vähendavad riski tõenäosust ja mõju. Need võivad olla tehnilised (turvalised infosüsteemid), õiguslikud (andmevahetusleping volitatud töötlejaga) või korralduslikud (vajaduspõhine juurdepääs andmetele). Pärast riskide maandamist tuleks riske uuesti hinnata, kuni need on allapoole keskmist. Kui riski ei saagi täiesti maandada, tuleb kirjeldada seiretegevust selle pidevaks jälgimiseks ja maandamiseks kogu uurimistöö vältel. Seda nimetatakse **riskide haldamiseks** ja see eeldab valmidust ja võimekust tegutseda, kui mõni riskidest realiseerub või tuvastatakse mõni uus risk. Riskide haldamise eel tuleb kokku leppida, milline on eri osaliste vastutus, kes riske seirab ja kuidas neile reageeritakse.

Loe lisaks

- Euroopa Liidu Küberturvalisuse Ameti (ENISA, 2006) aruanne „Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools“
- Euroopa Komisjoni (2021) suunis „EU Grants: How to complete your ethics self-assessment“, kus nähakse ette riskide hindamise vajadus keskkonna kahjustamise, teadustöö ohutuse, tehisintellekti kasutamise, teadustulemuste väärkasutamise ja isikuandmete töötlemise kontekstis

2.14.2. Isikuandmete töötlemisega seotud ohtude hindamine

Üldistel teaduseetilistel riskidel võib olla ühisosa andmekaitseohtudega[5] – näiteks võidakse uuringu tegemisel kahjustada inimeste õigust privaatsusele või neid diskrimineerida. Seega tuleb teadlasel enne teadustööga alustamist välja selgitada, milline oht isikuandmete töötlemisega kaasneb ja milline on selle võimalik mõju inimestele.

Andmekaitsega seoses tuleks kaaluda ohte vähemalt kahel juhul.

Esiteks tuleb hinnata **infoturberiske**, et tagada isikuandmete terviklus, käideldavus, konfidentsiaalsus ja turvaline töötlemine. Enamasti tegelevad sellega ülikooli infoturbespetsialistid, kes kindlustavad teadlastele sobivad töövahendid (vt alaptk 3.1).

Teiseks peab arvestama isikuandmete töötlemisel tekkiva **võimaliku kahjuga** andmesubjektidele. Kui uuringuga kaasneb suur risk kahjustada inimeste õigusi ja vabadusi, on vastutaval töötajal üldmääruse kohaselt kohustus koostada **andmekaitsealane mõjuhinnang**, mis on üks riskide hindamise erivorme.

2.14.3. Andmekaitsealase mõjuhinnangu koostamine

Andmekaitsealase mõjuhinnangu koostamine on vajalik juhul, kui isikuandmete töötlemine – võttes arvesse isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke – tõenäoliselt ohustab inimeste õigusi ja vabadusi. Puudub ühene ja lihtne määratlus, millal on mõjuhinnang kohustuslik – vastutav töötleja peab ise hindama kavandatava töötlemise mõju inimestele.

Andmekaitses on tähtsal kohal suure ohu mõiste. Üldmääruses ja Andmekaitse Inspektsiooni juhendites on aga isikuandmete suure ohuga töötlemist määratletud veidi erinevalt.

1. **Üldmääruses** on toodud kolm näidet suure ohuga andmetöötlusest:
   - inimeste süsteemne, ulatuslik ja automatiseeritud hindamine või jälgimine (sh profiilianalüüsi koostamine), millel on inimestele õiguslikud või muud samaväärse mõjuga tagajärjed;
   - eriliiki või süütegudega seotud isikuandmete ulatuslik töötlemine;
   - avalike alade ulatuslik jälgimine.

Nendel juhtudel on mõjuhinnangu tegemine kohustuslik. Muudes olukordades tuleb vastutaval töötlejal ohu suurust ise hinnata. Oluline on seejuures kahju inimeste õigustele ja vabadustele – kui esineb arvestatav tõenäosus inimeste õiguse ja vabadusi kahjustada, ongi tegemist suure ohuga.

2. **Andmekaitse Inspektsioon** on seadnud andmekaitsealase mõjuhinnangu tegemisele lisakriteeriumid – töötlemise **ulatuslikkus** ja **süsteemsus**. Andmekaitse Inspektsiooni isikuandmete töötleja üldjuhendi 5. peatüki järgi on andmetöötlus süsteemne, kui see on metoodiline ja planeeritud. Kuna teadustöö on vaikimisi alati süsteemne, tuleb vastutaval töötlejal suure ohu hindamisel pöörata tähelepanu eelkõige töötlemise ulatuslikkusele, sealjuures nii kvantitatiivselt (suur andmesubjektide arv) kui ka kvalitatiivselt (eriliiki ja süüteoandmed).

[5] Ehkki IT-, riigikaitse-, keskkonna- ja mõnes muus valdkonnas on tavaks pidada *riski* ja *ohtu* eri mõisteteks (vt nt https://akit.cyber.ee/term/52-risk ja https://akit.cyber.ee/term/93-oht, https://eits.ria.ee/et/seletav-sonaraamat/o?id=96649ad7b153a7f6d3bae608d0b1cbfe, https://sonaveeb.ee/search/unif/dlall/mil/risk/1 ja https://sonaveeb.ee/search/unif/dlall/mil/oht/1, https://www.riigiteataja.ee/akt/163255), on need terminid siin juhendis eri õigusaktide ja juhendite sõnastuse tõttu kasutusel sünonüümidena.

Andmekaitse Inspektsioon on kirjutises „Mõjuhinnangu tegemine“ täpsustanud, millal kaasneb töötlemise ulatuslikkusega nii suur oht, et andmekaitsealane mõjuhinnang on vajalik:

- 5000 ja enama inimese eriliiki või süüteoandmete töötlemisel;
- 10 000 ja enamale inimesele suurt ohtu põhjustavate andmete töötlemisel;
- muudel juhtudel 50 000 ja enama inimese andmete töötlemisel.

Need arvud puudutavad Eestis toimuvat isikuandmete töötlemist. Kui teadusuuringus töödeldakse andmeid piiriüleselt, tuleb ulatuslikkuse kriteeriumit hinnata juhtumipõhiselt.

Suur oht kaasneb Andmekaitse Inspektsiooni juhendite kohaselt näiteks siis, kui töödeldakse

- andmeid, mille avalikuks tulek rikub sõnumisaladust;
- inimeste asukohaandmeid reaalajas;
- isikuandmeid viisil, mis võib inimestele kaasa tuua õigusliku mõjuga diskrimineerimise;
- laste isikuandmeid.

Andmekaitsealase mõjuhinnangu sisu

Andmekaitsealane mõjuhinnang koosneb üldmääruse artikli 35 kohaselt neljast suuremast osast:

- kavandatud andmetöötlustoimingute ja nende eesmärkide kirjeldus;
- kavandatud toimingute vajalikkuse ja proportsionaalsuse hinnang;
- inimeste õigusi ja vabadusi puudutava ohu hinnang;
- ohu maandamiseks võetavate meetmete kirjeldus.

Mõjuhinnangu koostamisel tuleb abiks võtta teised otseselt uuringuga seotud isikuandmete töötlemist puudutavad dokumendid, näiteks uuringu protokollid, mis kajastavad andmetöötluse meetodit, juurdepääsuõiguste andmise põhimõtted, lepingud jms. Vajaduse korral tuleb kaasata andmekaitsespetsialist. Rahvusvahelise teadusuuringu puhul võib selle korraldaja seada nõude koostada tema eeskirjade alusel asukohariigis mõjuhinnang.

Andmekaitse peaspetsialist tuleb kindlasti kaasata siis, kui mõjuhinnangu tulemusena leitakse, et suur oht püsib ja kavandatud meetmed ei aita seda täielikult kaotada või piisavalt maandada. Koostöös otsitakse maandamisvõimalusi ja vajaduse korral saab pidada nõu Andmekaitse Inspektsiooniga.

Loe lisaks

- Andmekaitse Inspektsiooni isikuandmete töötleja üldjuhendi 5. peatükk „Andmekaitsealane mõjuhinnang“ ja lisa 1 „Mõjuhinnangu tegemise kontrollnimekiri“
- Euroopa Liidu Küberturvalisuse Ameti (ENISA, 2006) aruanne „Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools“
- Andmekaitse Inspektsiooni näidis mõjuhinnangust

2.15. Mida pidada silmas laste isikuandmete töötlemisel?

Üldmääruse kohaselt vajavad laste isikuandmed tavapärasest suuremat kaitset. Alaealisel on enda andmete üle täpselt samasugused õigused kui täiskasvanutel, kuid piiratud teovõime tõttu ei saa ta anda nõusolekut enda isikuandmete töötlemiseks. Nii ÜRO lapse õiguste konventsiooni kui ka lastekaitseseaduse kohaselt on teadlastel kohustus seada lapsi puudutavais otsustes alati esikohale lapse huvid. Seega peab alati arvestama, mida lapsed soovivad või eelistavad, isegi kui nende vanemad või eestkostjad on lapse eest nõusoleku andnud.

2.15.1. Alaealine ei saa anda nõusolekut, kuid ta peab oma andmete töötlemisega nõustuma

Isikuandmete kaitse õigusnormistik eeldab, et lepingu allkirjastajal või nõusoleku andjal on esindusõigus. Eesti seadused peavad teovõimeliseks vähemalt 18-aastast inimest, mistõttu on alaealise puhul vajalik tema vanema või muu seadusliku esindaja nõusolek. Seadusega on siiski võimalik alaealiste teovõimet laiendada: näiteks on IKS-i § 8 kohaselt vähemalt 13-aastasel lapsel õigus anda iseseisvalt nõusolek infoühiskonna teenuse (nt sotsiaalmeedia) kasutamiseks. Teadusuuringute jaoks ei ole sellist erandit tehtud ja infotehnoloogiliste lahenduste kasutamine isikuandmete kogumiseks ei muuda uuringut infoühiskonna teenuseks.

Siiski tuleb üldmääruse kohaselt arvestada alaealiste õigusi: neile tuleks anda teavet isikuandmete töötlemise kohta ja nende vaba tahet tuleb austada. Teadusuuringute puhul on hea tava paluda alaealistel enda uurimisega nõustuda (ingl *assent*), isegi kui see ei ole õiguslikus mõttes nõusolek. Kui alaealine ei nõustu enda isikuandmete töötlemisega, ei ole tema uuringusse kaasamine lubatud, isegi kui vanem on selleks nõusoleku andnud. Tahtevastane kaasamine on vastuolus hea teadustavaga ning isikuandmete õiglase töötlemise põhimõttega. Sama kehtib juhul, kui alaealine soovib ise oma nõustumist tagasi võtta, kuid tema vanem pole nõusolekut tagasi võtnud – õiglane töötlemine ja lapse autonoomia austamine eeldavad teadlaselt lapse sooviga arvestamist.

2.15.2. Lapsele tuleb anda teavet tema andmete kasutamise kohta lihtsas ja selges keeles

Nõusolekul põhinevate uuringute puhul tuleb anda teavet ka lastele, kellele võib koostada eraldi teabevormi. See peab olema eakohases sõnastuses või vormistatud piltide, ikoonide või animatsioonide abil. Ühtlasi võiks olla lastele tagatud lihtne võimalus esitada küsimusi.

Loe lisaks

Iirimaa Andmekaitsekomisjoni 2021. aasta aruanne „Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing“, milles antakse soovitusi lapse huvidega arvestamiseks ja lastele teabe edastamiseks

2.15.3. Lapse isikuandmete töötlemise õiguslik alus ei saa olla õigustatud huvi

Kuigi õigustatud huvi on teadustöös erandlik, ei keelata üldmääruses otsesõnu laste isikuandmete töötlemist õigustatud huvi alusel. Siiski eeldab see lapse huvide ja õiguste kaalumist. Üldmääruse rõhutus annab mõista, et õigustatud huvi kaalumisel on lapse õigused ja huvid tavapärasest tähtsamad.

2.16. Mida pidada silmas surnud isikute andmete töötlemisel?

Inimese surm on andmekaitse seisukohalt keeruline teema, kuna ei üldmääruses, IKS-i seletuskirjas, Euroopa Andmekaitsenõukogu ega Andmekaitse Inspektsiooni juhistes ei käsitleta seda, mis saab isikuandmetest pärast inimese surma.

Üldmäärus kaitseb vaid elus inimeste andmeid ja seepärast on liikmesriikidel võimalus ise surnute andmete töötlemist piirata.

IKS-i §-s 9 on täpsustatud surnud isikute andmetöötluse erisusi. Surnud täiskasvanu andmed on kaitstud 10 aastat ja alaealiselt surnute andmed 20 aastat pärast surma. Selle aja jooksul tuleb järgida kõiki andmekaitsepõhimõtteid, sh leida töötlemiseks sobiv õiguslik alus. Pärast seda andmekaitse enam nendele andmetele ei laiene ning nende kasutamisel tuleb lähtuda üldistest teaduseetika põhimõtetest ja erialastest tavadest.

2.16.1. Surnud isikute andmete kaitse eesmärk on kaitsta teisi inimesi

Surnud inimese andmed võivad puudutada ka tema lähedasi. Seepärast tuleb meeles pidada, et kaitsmise keskmes ei ole mitte surnud inimese, vaid tema lähedaste huvid ja õigused. Kui teadlasel on ligipääs surnud isiku toimikule, dokumentidele, päevikutele või muudele materjalidele, on neis sisalduvate elus inimeste andmed endiselt kaitstud.

Näiteks võib keeruliseks osutuda surma asjaolude andmete töötlemine juhul, kui surma on põhjustanud elus inimene või kui surma põhjuse alusel saab teha järeldusi ka teiste inimeste tervise kohta. Samuti võib olla piiratud teabe kasutamine muudel alustel, näiteks kui sellest võib ilmneda lapsendamissaladus perekonnaseaduse § 164 tähenduses.

2.16.2. Pärast surma läheb nõusoleku andmise ja tagasivõtmise õigus pärijatele

Nõusolekupõhiste uuringute puhul tuleb arvestada, et surnud inimese andmete töötlemise nõusoleku saab anda pärija. Kui andmeid on kavas koguda surmajärgse kümneaastase kaitseaja jooksul, tähendab see teadlasele lisavaeva, sest ta peab välja selgitama pärijad ja nendega ühendust võtma. Mitme pärija korral saab nõusolekut anda ja tagasi võtta ükskõik milline neist. Pärijate puudumisel lähevad pärandatavad õigused pärimisseaduse § 18 lg 1 alusel üle andmesubjekti kodukoha omavalitsusele, kellelt saab nõusolekut küsida. Kui on ette teada, et surnud isiku andmete kogumisel on nõusoleku küsimine keeruline, võib kaaluda, kas on võimalik kasutada muud õiguslikku alust.

2.16.3. Muud andmesubjekti õigused pärijatele üle ei lähe

Mõnevõrra keerulisem küsimus puudutab seda, kuivõrd saavad pärijad kasutada üldmääruse kolmandas peatükis loetletud andmesubjekti õigusi. Kuna nõusoleku tagasivõtmisel võib surnu isikuandmete töötlemine osutuda ebaseaduslikuks, võiks sellest omakorda järeldada, et pärija võiks esitada ka üldmääruse artikli 17 kohase taotluse andmete kustutamiseks. Samas ei ole IKS-i seletuskirjas mainitud, kas ja kuivõrd on võimalik pärida muid andmesubjekti õigusi oma andmete suhtes. Kui pärija peaks siiski esitama taotluse andmete kustutamiseks, on võimalik toetuda üldmääruse artikli 17 lg 3 punktis d nimetatud üldistele eranditele, milleks on avalikes huvides arhiveerimine, teadus- või ajaloouuringud (vt ka p 2.9.4).

2.16.4. Teadlasel ei ole kohustust pidada arvet uuritavate elu ja surma üle

Üldmääruse artikli 11 kohaselt ei ole vastutaval töötlejal kohustust koguda isiku tuvastamiseks lisaandmeid ainult selleks, et järgida üldmääruse nõudeid. Kuigi artiklis 11 ei räägita otseselt andmesubjekti elusolemise tuvastamisest, võib siiski oletada, et sarnane põhimõte laieneb ka sellele, liiati kuna üldmäärus surnud isikute andmeid ei kaitse. Seega võib eeldada, et teadlasel puudub kohustus pidada arvet, kes tema uuritavatest on elus ja kes on surnud, ainult selleks, et tuvastada, kellel on õigus nõusolek tagasi võtta. Pealegi võib sellises elusolemise pidevas jälgimises näha eraldiseisvat eesmärki, millel ei ole teadustöö eesmärkidega midagi ühist ja mis seetõttu vajaks eraldi põhjendamist.

Paratamatult võib seega juhtuda, et pärast andmesubjekti surma ei tea lähedased tema uuringus osalemisest midagi ja teadlased omakorda ei tea, et andmesubjekt on surnud. Sellistele olukordadele tuleb läheneda juhtumipõhiselt. Kui andmesubjekt on andnud nõusoleku enne surma, võib uuringuga jätkata, kuid kui lähedane soovib nõusoleku tagasi võtta, tuleb sellega arvestada. Sel juhul peab pärija tõendama, et andmesubjekt on surnud ja tema on pärija. Tõestamiseks sobib surmatõend, mida teadlane aga ei pea kusagil talletama.

Andmesubjekti võimaliku surmaga arvestamisel puuduvad selged tavad. Kui teadustööd planeerides on teada, et andmesubjektide surm on tõenäoline – näiteks uuritakse väga eakaid või surmavalt haigeid inimesi või uuritavad teevad väga ohtlikku tööd –, võib kaaluda lahendusi, kuidas teadustööga seotud teavet juba varakult lähedastele edastada.

2.16.5. Surnute andmeid võib muul õiguslikul alusel töödelda

Kui teadustöö toimub muul õiguslikul alusel peale nõusoleku, siis ei muuda andmesubjekti surm andmetöötluse seisukohalt kuigi palju. Surnud isikute andmete kümneaastane kaitse (alaealistel 20 aastat) kehtib vaid andmesubjekti nõusoleku olemasolul, mida surma järel saab anda ja tagasi võtta pärija. Kui õiguslik alus on näiteks avalikes huvides ülesanne, võib andmeid edasi töödelda ka ilma andmesubjekti ja pärija nõusolekuta (vt ka alaptk 2.4). IKS-i § 9 lg 4 annab erandkorras võimaluse töödelda ilma pärija nõusolekuta ka inimese nime, sugu, sünni- ja surmaaega, surma fakti, matmise aega ja kohta.

3. Teadustöö tegemine: andmete kogumine ja analüüs

Selles peatükis antakse ülevaade andmekaitse küsimustest, mis võivad ette tulla teadusuuringu käigus, kui isikuandmete töötlemine on juba alanud. Peatükis käsitletakse turvalisuse tagamist, anonüümimist, pseudonüümimist ja võimalikele rikkumistele reageerimist.

Vaatamata põhjalikule planeerimisele võivad ootamatud probleemid ilmneda ka teadustöö tegemise ajal. Samuti tuleb arvestada võimalusega, et uuringusse kaasatud isikud soovivad kasutada oma õigusi ja esitavad oma andmete kohta päringuid või muid nõudmisi.

3.1. Kuidas tagada, et isikuandmete töötlemine oleks turvaline?

Turvalisus tähendab isikuandmete puhul eelkõige andmete tervikluse, käideldavuse ja konfidentsiaalsuse tagamist. Turvalisust aitavad kindlustada nii tehnilised vahendid (nt seadmed, tarkvara) kui ka töökorralduslikud meetmed (nt juurdepääsuõigused, koolitused). Turvalisuse püsimise tagamiseks tuleb aeg-ajalt uuesti hinnata, kas kasutatavad vahendid ja meetmed on piisavad. Näiteks viie aasta taguse teadusprojekti jaoks võetud meetmed ei pruugi enam olla uues projektis piisavad.

Isikuandmete **terviklust** ohustab kogu tegevus, mille käigus andmeid volitamata muudetakse või kustutatakse, näiteks vargused, küberründed, seadmete ja süsteemide tehnilised vead või õnnetused. Teadustöö puhul võib see tähendada isegi uuringu luhtumist, sest andmeid pole enam piisavalt või neid ei saa analüüsida. Terviklust võivad kahjustada ka hooletusvead, kui teadlased muudavad või kustutavad kogemata andmeid. Selliste vigade eest aitab kaitsta varundamine ja andmetöötlustarkvara, mis analüüsi käigus alusandmeid ei muuda.

Käideldavus eeldab, et isikuandmed on oma kogumise eesmärgi jaoks hõlpsasti kasutatavad. Näiteks võib andmete talletamine võrguühenduseta seadmes olla küll turvaline, kuid see võib märgatavalt vähendada nende käideldavust, kui teadlased peavad andmete analüüsimiseks iga kord kuskile füüsiliselt kohale minema. Samas ei ole kõige mugavamad ja populaarsemad töövahendid alati kõige turvalisemad. Seega tuleb püüda leida sobiv kompromiss.

Isikuandmete **konfidentsiaalsust** kahjustab see, kui eraeluline teave saab teatavaks kõrvalistele inimestele, kellele andmeid ei ole mõeldud. Näiteks ilma arvutit või tööruumi lukustamata oma töökohalt lahkudes või avalikus kohas (ühissõidukid, kohvikud, pargid) sülearvutis või telefonis töötades võivad lähedal olevad inimesed näha isikuandmeid sisaldavaid faile. Selliseid probleeme aitavad ennetada eelkõige töökorralduslikud meetmed. Veel suurem ohuallikas on pahatahtlikud ründed, mille eesmärk on isikuandmeid varastada või lekitada. Seepärast on hea isikuandmed pseudonüümida, siis on andmete lekkimise või vargusega kaasnev kahju inimeste eraelule väiksem.

Allpool on kommenteeritud mõnda Euroopa Andmekaitsenõukogu suunises 4/2019 üldmääruse artikli 25 „Lõimitud andmekaitse ja vaikimisi andmekaitse“ kohta esitatud nõuannet ja selgitatud, kuidas täita neid teadustöö puhul.

3.1.1. Infoturbe süsteemne haldamine

Süsteemse infoturberiskide hindamise ja turvameetmete rakendamise, seire ja täiustamisega tegeleb eelkõige Tartu Ülikool. Samuti on tema ülesanne tagada, et teadlastele pakutavad infosüsteemid,

töövahendid ja teenused oleksid isikuandmete töötlemiseks piisavalt turvalised. Süsteemsus eeldab ka andmekaitseriskide hindamist ja haldamist (vt ka alaptk 2.14).

Teadlase ülesanne on infoturbe ohte teadvustada, järgida kokkuleppeid ja juhiseid ning küsida vajaduse korral abi. Abiks on ülikooli koostatud küberturbe juhised.

3.1.2. Vajaduspõhine juurdepääs isikuandmetele

Juurdepääsuõiguste haldamine on üks tavapärasemaid turvameetmeid, mida vastutav töötleja võib rakendada. Juurdepääsu piiramise eeldus on selge ülevaade teadlastest, kellel on tarvis isikuandmeid teadustöö eesmärgil töödelda. Oluline on tagada, et need, kellel puudub vajadus isikuandmeid töödelda, ei saaks seda tahtlikult või kogemata teha. Kui teadustöö mingis etapis kaasatakse üliõpilasi, tuleb nendega sõlmida konfidentsiaalsusleping.

Juurdepääsuõiguste kontrollimiseks võib olla vaja logifaile säilitada, eriti kui tegemist on pikemaajalise uuringuga, mille raames töödeldakse suures koguses tundlikke andmeid. Samuti tasub juurdepääsuõigustele rohkem tähelepanu pöörata juhul, kui on teada, et uuringumeeskonna liikmed vahetuvad tavapärasest sagedamini.

3.1.3. Andmete turvaline edastamine

Kui isikuandmeid on vaja edastada teisele teadlasele või teadusasutusele, tuleb tagada, et nende terviklus ega konfidentsiaalsus ei saaks selle käigus kahjustada. Näiteks tuleks võimaluse korral vältida isikuandmetest koopia edastamist e-kirjaga, kui andmesaajale on võimalik luua juurdepääs infosüsteemi kaudu, kus andmed asuvad. Kui e-posti teel saatmine on ainuvõimalik lahendus, tuleks andmed krüpteerida või kasutada muid meetmeid, vältimaks võimalust, et andmeid võib näha keegi muu peale adressaadi.

Turvarisk on näiteks isikuandmete edastamine mälupulga või muu välise andmekandja kaudu, mis võib minna kaduma. Kui seda siiski tehakse, peaks turvalisuse tagamiseks olema krüpteeritud nii andmekandja kui ka sellel asuv andmefail.

3.1.4. Andmete turvaline talletamine

Andmete talletamisel tuleb kaitsta neid volitamata muudatuste ja juurdepääsu eest. See sõltub teadlase võimalustest ja kasutatavatest vahenditest:

- ülikooli teadustööks kogutud isikuandmete talletamiseks tuleb kasutada ainult ülikooli tööarvutit. Tavaliselt on selleks sülearvuti, mille teadlane võtab kaasa tööle, lähetusse ja koju. Vältida tuleb olukorda, kus kõrvalised isikud pääsevad tundlikke andmeid sisaldavasse tööarvutisse;
- ülikool ei saa vastutada andmetöötluse eest, mis on teadlase isiklikus arvutis. Kui eraarvuti kasutamisel saavad andmed avalikuks (andmekaitsealane rikkumine), vastutab teadlane andmesubjektide ja ülikooli ees, peab heastama andmesubjektidele tekkinud olukorra ning andma aru Andmekaitse Inspektsioonile;
- võrku ühendamata seade on turvalisem kui võrku ühendatud seade, kuna selle ründamine on märksa keerulisem;
- ühe kasutajaga seade on turvalisem kui mitme kasutajaga seade.

Isikuandmete turvalisel talletamisel on veel mitu kriteeriumi, mida tuleb arvesse võtta, näiteks andmete tundlikkus, hulk, käideldavus, juurdepääsu haldamise võimalus, töötlemiseks kasutatavad seadmed ja tarkvara.

3.1.5. Andmete varundamine

Varundamine aitab tagada andmete tervikluse ja käideldavuse juhul, kui need hävivad õnnetuse, pahatahtliku tegevuse või hooletuse tõttu või saavad märkimisväärselt kahjustada. Andmehalduses on käibel 3-2-1-reegel: andmeid tuleks varundada vähemalt kolmes eksemplaris, vähemalt kahel eri andmekandjal või keskkonnas, sealjuures üks andmekandja peaks asuma mujal.

Kolmest eksemplarist üks võiks olla tööeksemplar, milles saab töö vältel andmeid muuta, täiendada ja kustutada. Teine eksemplar on vajalik juhuks, kui tööfail saab kahjustada, sealt kustutatakse kogemata olulised andmed või see hävineb. Kolmas eksemplar on varundatud koopia, mis asub teises seadmes või keskkonnas (pilves vm) ega ole lihtsasti kättesaadav. Näiteks võib hoida andmeid lisaks tööseadmele ka ülikooli võrgukettal, serveris või pilvekeskkonnas. Pilveteenust kasutades tuleb veenduda, et ülikoolil on sõlmitud selle keskkonnaga leping. Kui hoida andmeid kahel eri andmekandjal, aitab see tagada, et kui ühega midagi juhtub (tulekahju, uputus, vargus vm), jäävad andmed teise andmekandjasse alles. Sel juhul tuleb osata riske hinnata: näiteks ei pruugi tulekahju eest kaitsta see, kui varukoopia asub sama hoone teises ruumis.

Samal ajal peab varundamine olema läbimõeldud, eesmärgipärane ja kooskõlas andmekaitse minimaalsuse põhimõttega. Igaks juhuks (selge eesmärgi ja vajaduseta) andmeid dubleerida ei või. Varundamise kohta saab nõu ja abi e-posti aadressil arvutiabi@ut.ee.

Loe lisaks

Tartu Ülikooli raamatukogu andmehaldusplaani koostamise juhendi peatükk „Andmete turvaline säilitamine teadustöö vältel“

3.1.6. Teadlikkus rikkumisvõimalusest

Rikkumine on isikuandmete väärkasutamine (avalikustamine, kustutamine, nõusoleku küsimisel tehtavad eksimused jm). Rikkumisi aitab ära hoida see, kui teatakse peamisi teadustöö andmekaitsepõhimõtted ja võimalikke riske. Ennetustöö nõuab märksa vähem ressursse kui tegelemine rikkumise tagajärgedega.

Rikkumisest tuleb viivitamata teavitada andmekaitse peaspetsialistile e-posti aadressil andmekaitse@ut.ee (vt ka alaptk 3.5).

3.1.7. Isikuandmete töötlemiseks sobivad teenused, tarkvara ja vahendid

Isikuandmete töötlemisel kasutatavad töövahendid peavad tagama isikuandmete turvalise töötlemise, konfidentsiaalsuse, käideldavuse ja tervikluse, samuti andmesubjekti õiguskaitse. Seega saab töövahendeid eristada selle alusel, kas töötlemise käigus pääseb andmetele juurde ainult töötleja või ka töövahendi looja ja teenusepakkuja, nt küsitluskeskkonna omanik, repositooriumi haldaja või tarkvara litsentseeriv ettevõte.

Kui andmed liiguvad ülikoolist väljapoole, tuleb hoolega hinnata, kas töövahend sobib teadustööks. Selleks tuleb tutvuda teenusepakkuja või tarkvara omaniku andmekaitsetingimustega. Kui andmete

töötlemist ei kirjeldata seal piisavalt põhjalikult või need tekitavad kahtlusi, ei ole see ilmselt usaldusväärne teenus ega tarkvara.

Küsimuste või kahtluste korral tuleb pidada nõu ülikooli infoturbejuhiga. Mõnikord on võimalik teenusepakkujaga sõlmitavas lepingus õiguslikud ja tehnilised riskid maandada, leppides näiteks kokku, et andmeid säilitatakse vaid ülikooli serverites.

Pakutavad teenused ja tarkvara võivad toimida kolmel viisil.

- **Need ei edasta isikuandmeid**: sellised lahendused on alati turvalisemad, kuna töödeldavad andmed püsivad vaid ühes seadmes või infosüsteemis, mida teadlane kasutab. Näiteks kvalitatiivsete andmete analüüsi tarkvara säilitab tavaliselt intervjuude transkriptsioonid teadlase enda seadmes ja andmeid kuhugi ei edasta. Sellisel juhul sõltub turvalisus teadlase enda tegevusest, sealhulgas sellest, kus ja kuidas ta intervjuude salvestisi, transkriptsioone või nende osi hoiab. Arvestada tuleb, et tarkvara enda loodud projektifailid võivad sisaldada isikuandmeid.
- **Need edastavad isikuandmeid teadusasutuse piires**: selline lahendus on näiteks ülikooli hallatav pilveteenus või mõnelt ettevõttelt litsentseeritud tarkvara, mille puhul on tagatud andmete hoidmine vaid ülikooli süsteemides. Siin tuleb meeles pidada, et lahenduse turvalisuses peab veenduma teadlane.
- **Need edastavad isikuandmeid teadusasutusest väljapoole:** sellisel juhul tuleb veenduda piisavas turvalisuses ja õiguslikus kaitses. Eriti valvas tuleks olla lahenduste puhul, kus isikuandmed liiguvad automaatselt Euroopa Liidust väljapoole, näiteks kui kõiki sisestatud andmeid hoitakse serverites, mis asuvad kolmandates riikides (vt alaptk 3.2). Sellisel juhul on üldiselt vaja lisakaitsemeedet, näiteks lepingut ülikooli ja teenusepakkuja vahel. Kui andmeid hoitakse mõnes Euroopa Liidu liikmesriigi serveris, pakub see piisavat õiguslikku kaitset, kuid veenduda tuleb, et seda tehakse turvaliselt.

3.2. Mida pidada silmas, kui isikuandmeid edastatakse ühest riigist teise?

Riikidevahelisel andmete liikumisel kehtib üldine põhimõte, et sihtriigis peab olema tagatud piisav andmekaitse tase. Teatud riikide puhul peetakse kaitset piisavaks, teiste puhul on Tartu Ülikoolil kui vastutaval töötlejal kohustus võtta lisameetmeid. Seepärast tuleks näiteks kolmandatesse riikidesse isikuandmete edastamise soovi korral pidada alati nõu ülikooli andmekaitse peaspetsialistiga.

3.2.1. Euroopa Liidu liikmesriigid, Island, Liechtenstein ja Norra

Kui isikuandmeid edastatakse Euroopa majanduspiirkonna riikidesse, on piisav kaitse tagatud üldmäärusega ja sellisel juhul ei teki ühtki lisapiirangut ega -nõuet. Järgida tuleb üldpõhimõtteid: töötlemine peab olema seaduslik, õiglane, läbipaistev, turvaline, eesmärgipärane ja minimaalne. Samuti peab andmete edastamiseks olema sõlmitud leping.

Siiski on teadustööd ja teaduseetikat puudutav eri EL-i liikmesriikide seadustes mõnevõrra erinevalt reguleeritud. Seetõttu on soovitatav partneritega arutada, millised isikuandmetega seotud nõuded teises riigis kehtivad.

3.2.2. Piisava andmekaitse tasemega kolmandad riigid

Kui andmeid saadetakse Euroopa majanduspiirkonna välisesse ehk kolmandasse riiki, tuleb hinnata sealse andmekaitse taset. Euroopa Komisjon on leidnud, et andmekaitse on piisav Andorras, Argentinas, Kanadas, Fääri saartel, Iisraelis, Jaapanis, Korea Vabariigis, Šveitsis, Uruguays, Uus-Meremaal, Ühendkuningriigis ja Briti krooni sõltkondades Guernsey, Mani ja Jersey saarel. Seal ei ole lisakaitsemeetmed vajalikud ja kehtivad samad nõuded mis EL-i liikmesriikide puhul.

Loe lisaks

Piisava andmekaitsetasemega riigid Euroopa Komisjoni veebilehel

3.2.3. Muud kolmandad riigid

2016. aastal hindas Euroopa Komisjon EL-i–USA andmekaitseraamistiku Privacy Shield kaitsetaseme poolest piisavaks, kuid Euroopa Kohtu 2020. aasta otsusega see hinnang tühistati – seega ei ole Ameerika Ühendriikide andmekaitse tase praegu piisav. Eesti ja USA vaheline isikuandmete vahetus vajab seepärast lisakaitsemeetmeid. Selleks sobib näiteks USA-s asuva asutusega sõlmitav andmete edastamise leping või mõni muu üldmääruse artiklis 46 nimetatud meede. Lisaks tuleb isikuandmete saatmisel USA-sse teha andmekaitsealane mõjuhinnang (vt p 2.14.3).

Ka kõigi muude kolmandate riikide puhul, mille andmekaitse taset ei ole Euroopa Komisjon piisavaks tunnistanud, tuleb vastutaval töötlejal rakendada lisakaitsemeetmeid, mis tähendab enamasti kolmandas riigis asuva koostööpartneriga eraldi lepingu sõlmimist.

3.3. Miks ja kuidas isikuandmeid pseudonüümida?

Üldmääruse artikli 4 kohaselt on pseudonüümimine „isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga, tingimusel et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava füüsilise isikuga seostamise vältimise tagamiseks võetakse tehnilisi ja korralduslikke meetmeid“. Seega asendatakse pseudonüümimisel kõik inimese otsest või kaudset tuvastamist võimaldavad andmed ehk identifikaatorid pseudonüümiga, misjärel ei ole ta enam tuvastatav.

Siiski on pseudonüümimine tagasipööratav. Üldmääruses nimetatud täiendava teabe – võtme, koodi või muu tuvastamist võimaldava info – abil saab taastada algupärase seose andmete ja isiku vahel. See täiendav teave võib kõige lihtsamal kujul olla näiteks tabel inimese tuvastamist võimaldavatest andmest ja nende asendamiseks määratud pseudonüümidest. Turvalisuse tagamiseks peab seda teavet hoolega kaitsma.

Niisiis on *pseudonüümimine* üldmõiste kõigi andmetöötlusmeetodite kohta, mis võimaldavad nii isiku deidentifitseerimist (umbisikustamist) kui ka reidentifitseerimist (taasisikustamist). Ei tohi unustada, et pseudonüümitud andmed on endiselt isikuandmed. Isegi kui teadlased ei suuda andmetele peale vaadates isikut tuvastada, tuleb neid andmeid kohelda samamoodi kui tuvastamist võimaldavaid andmeid ja järgida tuleb kõiki andmekaitsepõhimõtteid.

Eesti õigusruumis valitsevad pseudonüümitud andmete kohta eri arusaamad. Näiteks on Andmekaitse Inspektsioon juhtinud tähelepanu IGUS-e § 7 muutmise vajaduse kohta. Nimelt sätestatakse selles: „Pseudonüümitud koeproovide, pseudonüümitud DNA kirjelduste ja pseudonüümitud terviseseisundi kirjelduste töötlemise suhtes ei kohaldata isikuandmete töötlemist reguleerivaid sätteid juhul, kui

koeproove, DNA kirjeldusi või terviseseisundi kirjeldusi töödeldakse hulgana ja tingimusel, et töödeldavaid proove või kirjeldusi on üheaegselt vähemalt viie geenidoonori kohta.“ Ent üldmääruse põhjenduses 26 on öeldud, et pseudonüümitud andmeid tuleks käsitleda teabena tuvastatava füüsilise isiku kohta. Seega ei saa pseudonüümitud geneetilisi ega terviseandmeid liigitada isikustamata andmeteks, millele üldmäärus ega IKS ei kohaldu.

3.3.1. Andmete pseudonüümimise põhjused ja aeg

Üldmääruse kohaselt suurendab pseudonüümimine isikuandmete töötlemise turvalisust ja lõimitud andmekaitset. Sealjuures tuleb järgida minimaalsuspõhimõtet: kui töötlemise käigus ei ole vaja teada isikut, kelle kohta andmed käivad, ei ole põhjendatud ka isikustatud andmete töötlemine. Seega ei puuduta pseudonüümimine vaid isikuandmete edastamist, vaid ka ühe teadusasutuse tööd või teadusprojekti, et vähendada nende teadlaste hulka, kes saavad andmete põhjal inimesi tuvastada.

Mida tundlikumad on andmed, seda vajalikum võib olla pseudonüümimine. Samuti tuleks seda kaaluda siis, kui andmeid edastatakse kolmandatele isikutele.

Isikuandmed tuleks pseudonüümida esimesel võimalusel. Näiteks mitme välismaise partneriga teadusprojektis tuleks seda teha vahetult pärast andmete kogumist ja enne analüüsiga alustamist või andmete edastamist projektipartneritele.

3.3.2. Andmete pseudonüümijad

Nagu on öeldud Euroopa Liidu Küberturvalisuse Ameti (ENISA) 2019. aasta juhendis pseudonüümimisvõtete ja parimate tavade kohta, võib pseudonüümijaks olla kas vastutav töötleja, volitatud töötleja või usaldusväärne kolmas isik. Andmete töötlemise turvalisuse tagab aga alati vastutav töötleja.

Pseudonüümimine on kindlasti vajalik mitme asutuse ühise teadusuuringu puhul. Näiteks võivad kaks või enam partnerit olla kaasvastutavad töötlejad, kuid neil tuleb leppida kokku, et isikuandmeid koguv teadusasutus pseudonüümib andmed enne kaasvastutavatele partneritele edastamist. Sel viisil järgitakse andmetöötluse minimaalsus- ja turvalisuspõhimõtet. Samuti võib isikuandmed pseudonüümida volitatud töötleja (nt küsitlusettevõte), enne kui ta need teadusasutusele üle annab.

3.3.3. Andmete pseudonüümimise meetodid

Asutuse või projektipõhiste pseudonüümimispõhimõtete kehtestamisel võib lähtuda ENISA juhendist pseudonüümimisvõtete ja parimate tavade kohta, kus soovitatakse pseudonüümimismeetodi valikule läheneda riskipõhiselt. Riskidena võetakse arvesse võimalikke ründeid pseudonüümitud andmestikele, andmete tundlikkust, käideldavust ja nende kaitsmise vajadust.

Enamasti ei piisa pseudonüümimiseks vaid inimese nime ja isikukoodi asendamisest pseudonüümiga, vaid kaaluma peab kõiki andmeid, mis on temaga lihtsasti seostatavad. Tähtis on ka andmete tüüp – näiteks ei sobi identifikaatorite pseudonüümimine kujutiste ja pildiliste andmete puhul, kuid see on kasulik, kui kujutiste failinimed või metaandmed sisaldavad identifikaatoreid, millel on isikute tuvastamist võimaldavad tunnused. Pseudonüümitud andmete töötleja ei tohi suuta andmete taga peituvaid isikuid tuvastada.

Identifikaatorite asendamiseks pseudonüümiga on eri viise:

- **loenduripõhisel pseudonüümimisel** kasutatakse määratud järjestuse alusel genereeritud numbreid identifikaatorite asendamiseks. Selle meetodi eelis on lihtsus ja see, et loenduri määratud numbril puudub otsene seos asendatava identifikaatoriga;
- **juhuarvude genereerimisel** asendatakse samuti identifikaatorid arvudega, kuid seda tehakse juhuslikult. Juhuarvud on loenduripõhisest meetodist turvalisemad, sest pseudonüüme ei genereerita järjestikku. Meetodi miinus on aga see, et kahele identifikaatorile võidakse määrata sama pseudonüüm. Selle tõenäosust saab vähendada, kui genereerida pikemaid numbreid;
- **krüptograafiline räsifunktsioon** võimaldab krüpteerida suvalise pikkusega identifikaatorid kindla pikkusega koodiks. Räsifunktsioon on ühesuunaline ehk pöördumatu, mis tähendab, et räsikoodi alusel on äärmiselt keeruline välja arvutada algset väärtust. Samuti on see kollisioonikindel ehk ei leidu kaht identifikaatorit, mis annavad tulemuseks sama räsikoodi. Et aga sama sisendi korral on tulemuseks sama räsi, on algset identifikaatorit ja räsifunktsiooni teades võimalik andmed depseudonüümida;
- **võtmepõhisel räsimisel** kasutatakse peale räsifunktsiooni salajast võtit pseudonüümide arvutamiseks. Võtmepõhine räsimine annab lisakindluse, et räsikoodi põhjal ei ole võimalik identifikaatorit välja arvutada;
- **sümmeetrilisel krüpteerimisel** kasutatakse krüpteerimiseks ja dekrüpteerimiseks ühtainust salajast võtit;
- väiksema andmestiku korral saab pseudonüüme luua ka **käsitsi**, näiteks asendada inimesega seotud identifikaatorid ja kvaasiidentifikaatorid[6] üldnimetusega *intervjueeritav A* või *uuritav M45*. Nimede asendamine initsiaalidega või mõne kvaasiidentifikaatori pesudonüümimine ei pruugi aga pakkuda tuvastamise eest kuigi tugevat kaitset. Juhuslikud pseudonüümid on pea alati turvalisemad kui süsteemipärased.

Olenemata meetodist on oluline kaitsta pseudonüümimise saladust – võtit, koodi, meetodit või muid andmeid, mis võimaldavad ühendada pseudonüümi isikuga. Kui see saladus küberründe tulemusena lekib, on võimalik tuvastada inimesed kõigis andmestikes, mis on pseudonüümitud kujul koostatud. Veelgi ohtlikum on selline rünne juhul, kui kasutatakse alati ühesugust pseudonüümimismeetodit. Sel juhul võib tekkida väga tõsine privaatsuse riive.

Saladuse hoidmiseks peaks juurdepääs depseudonüümimisteabele olema võimalikult vähestel inimestel, kuid neid peaks olema rohkem kui üks, et olla valmis olukorraks, kus teabe valdajaga midagi juhtub või kui ta töölt lahkub.

3.4. Miks ja kuidas isikuandmeid anonüümida?

Euroopa andmekaitse alases töörühmas anonüümimisvõtete kohta koostatud arvamuse nr 05/2014 kohaselt on anonüümimine andmete töötlemine pöördumatul viisil, st selle järel ei ole isikute taastuvastamine ühelgi mõistlikul ja tõenäolisel meetodil enam võimalik. Tänu sellele ei ohusta anonüümitud andmeid ka ründed: isegi kui kõik andmed langeksid ründajate kätte, ei ole neid võimalik isikustada. Seepärast ei ole anonüümitud andmed käsitatavad isikuandmetena.

[6] Kvaasiidentifikaator on sugu, vanus, rahvus või muu tunnus, mis eraldiseisvalt ei suuda isikut üheselt tuvastada, aga võimaldab koos teiste tunnustega luua otsese identifikaatori, mis viitab konkreetsele isikule.

Euroopa Andmekaitsenõukogu on leidnud suunises nr 04/2020 asukohaandmete ja kontaktide jälgimise vahendite kasutamise kohta Covid-19 puhangu kontekstis, et anonüümida saab vaid kogu andmestikku, mitte üksikuid andmelõike. Õiguslikus mõttes ei ole selge, millise tasemeni tuleb andmestikku töödelda, et pidada seda anonüümseks. Anonüümimismeetodid pakuvad kaitset eri määral ja sageli sõltuvad need konkreetsest andmestikust.

3.4.1. Andmete anonüümimise põhjused ja aeg

Isikuandmete anonüümimine aitab kaitsta inimeste privaatsust ja toetab minimaalsuspõhimõtet: kui teadustöö eesmärgid on saavutatavad anonüümitud andmetega, tuleks igal juhul eelistada anonüümimist.

Kuna anonüümitud andmeid ei loeta enam isikuandmeteks, on nende kasutamine ja jagamine vabam. Neid võib edastada teadusprojekti koostööpartneritele, talletada avaandmetena repositooriumides või saata muudele isikutele ja asutustele, kel on nende vastu huvi.

Anonüümitud andmete puhul on lihtsam tagada ka andmetöötluse turvalisus. Ainus risk, mida peab meeles pidama ja aeg-ajalt hindama, on võimalus, et tehnoloogia arenedes ja uute andmestike lisandudes võivad anonüümitud andmestikus olevad isikud uuesti tuvastatavaks muutuda.

Anonüümimisel väheneb pea alati andmete käideldavus. Kui andmed on mahukad, paljude muutujatega või kvalitatiivsed, võib anonüümimine takistada nende kasutamist või muuta need sootuks kasutuks, sest selle käigus moonutatakse andmeid. Näiteks sotsiaalteaduslike kvalitatiivsete andmete (intervjuude transkriptsioonid, tekstid) anonüümimine võib vähendada nende taaskasutamise võimalusi. Lisaks ei võimalda anonüümitud materjal isikuandmete põhjal tehtud teaduslikke analüüse korrata.

Andmeid saab ka kohe anonüümselt koguda, ent kui selle käigus salvestuvad kordumatud identifikaatorid (näiteks arvuti IP-aadress), on vajalik järeltöötlus, et välistada isikute kaudse tuvastamise võimalus. Seega tuleb hoolikalt hinnata, kas plaanitav meetod võimaldab koguda andmeid kohe anonüümselt või tuleb need anonüümida andmekogumise või teadustöö valmimise järel.

3.4.2. Andmete anonüümijad

Isikuandmete anonüümimise eest vastutab Tartu Ülikool, ent konkreetsete anonüümimistoimingute eest ülikooli teadlane, kellel on vajalikud teadmised, oskused ja vahendid. Anonüümijad võivad olla ka teadustööst väljapoole jäävad isikud, kui sellest on varem andmesubjekte teavitatud ning tagatud on sedalaadi anonüümimise seaduslikkus ja vastavus andmekaitsepõhimõtetele.

Teiseste andmete kasutamisel võib need anonüümida andmeid väljastav asutus.

3.4.3. Andmete anonüümimise meetodid

Anonüümimisviis sõltub suurel määral isikuandmete laadist ja hulgast. Seepärast tuleb hinnata, mil määral takistab valitud meetod andmete ja isiku seostamist ning kas see tulemus on pöördumatu.

Andmete anonüümimisel on levinud kolm peamist meetodit:

- **eemaldamise** käigus kõrvaldatakse või asendatakse jäädavalt kõik otsest tuvastamist võimaldavad tunnused (nimi, isikukood). Otseste identifikaatorite eemaldamine ei taga kohe anonüümsust, sest isikut saab tuvastada ka muude andmete põhjal: näiteks eristub ta kordumatu tunnuste kombinatsiooni tõttu või siis, kui eri andmestikud ühendatakse;
- **juhuslikustamine** ehk randomeerimine eeldab andmete juhuslikku moonutamist teatud väärtuste või tunnuste alusel. Andmete moonutamise tõttu ei pruugi randomeerimine

teadusandmete avaldamiseks sobida. See-eest kasutatakse juhuslikustamist suurte avalike andmestike kaitsmiseks taastuvastamise vastu;
- **üldistamise** käigus rühmitatakse väärtused tunnuste kaupa. Näiteks võib sünniaastad koondada vanusevahemikeks, palgasummad palgavahemikeks jne. Üldistamine aitab tagada, et isik ei ole tuvastatav, kuid selle miinus on see, et väärtuse täpsusaste väheneb.

Lisaks saab sõltuvalt anonüümitavatest andmetest eristada mõningaid erijuhte.

- **Andmestiku väljavõtte anonüümimine**

  Kuna anonüümimine peab olema pöördumatu, ei tohi jääda alles koopiat algandmetest, mida on võimalik anonüümitud andmestikuga taas ühendada. Siiski on võimalik teha andmestikust avalikustamiseks mõeldud anonüümitud väljavõtteid, nii et algandmed jäävad alles. Tehtud väljavõte ei tohi olla enam algandmetega ühendatav.

- **Pseudonüümitud andmete anonüümimine**

  Varem pseudonüümitud andmete anonüümimisel tuleb salajane võti kustutada. Lisaks tuleks hinnata pseudonüümimise piisavust: kui pseudonüümiga asendati vaid otsesed identifikaatorid, aga mitte andmete väärtused, võivad andmestikus esineda kordumatud kvaasiindikaatorite kombinatsioonid, mis lihtsustavad inimeste tuvastamist. Sellisel juhul tuleks lisaks võtme kustutamisele andmeid veel töödelda – näiteks üldistada –, et välistada kaudne tuvastusvõimalus. Korrektselt pseudonüümitud andmete puhul võib aga piisata võtme jäädavast kustutamisest.

Anonüümimismeetodit tuleb läbipaistvuse suurendamiseks isikuandmete omanikule täpselt kirjeldada, et ta saaks hinnata, kas ja kuivõrd ta peab sellist töötlemist piisavaks. Eriti vajalik on see juhul, kui anonüümitud andmed avaldatakse avatud teadusandmetena.

3.4.4. Andmete ja isikute seostamise vältimine

Et vähendada võimalust andmeid ja isikut seostada, tuleb vaadata andmestiku omadusi, näiteks andmete struktuuri, tüüpi või hulka. Näiteks vähendavad anonüümsust väga kitsa valimiga küsitlused, milles kogutakse paljude sotsiaalsete tunnuste kohta väga täpseid väärtusi või mis sisaldavad mahukaid vabatekstiga vastuseid. Euroopa Andmekaitsenõukogu suunises nr 04/2020 asukohaandmete ja kontaktide jälgimise vahendite kasutamise kohta Covid-19 puhangu kontekstis on käsitletud juhtumeid, kus andmeid on võimalik pärast anonüümimist isikuga seostada. Selle vältimiseks tuleb teada anonüümimise nõrku kohti.

- **Üksikisiku eristamise** (*singling out*) **võimalus** tekib siis, kui anonüümitud andmestikus esinevad kordumatud tunnused, näiteks IP-aadress, seadme ID või kvaasiidentifikaatorite kombinatsioon. Viimasel juhul on tarvis siiski lisasamme, et isik tuvastada, sest ühendada tuleb mitu sama isiku kohta käivat andmestikku.

Näide

Kui andmestikus esineb vaid üks sissekanne isiku kohta, kes on meessoost, vanuses 31–40, kõrgharidusega, töötab asutuse X allasutuses Y ning kelle staaž on 10 aastat, siis on ta üksikisikuna eristatav. Tema tuvastamiseks võib sel juhul piisata vaid sellest, kui asutuse X töötajate nimekiri koos piltide ja lühikeste elulookirjeldustega on avalik. Samuti suudavad selle isiku tuvastada ilmselt kõik sama asutuse töötajad.

Peamine meetod üksikisiku tuvastamise vältimiseks on ***k*-anonüümsus**, mis eeldab, et iga kvaasiidentifikaatorite kombinatsiooni kohta on andmestikus vähemalt *k* erinevat vastet. *K*-

anonüümsuse väärtus tuleb teadlastel endil valida sõltuvalt andmete tundlikkusest ja andmestiku eripäradest.

- **Andmete seostamise** (*linkability*) **võimalus** tekib juhul, kui kaks andmestikku saab mõningate tunnuste (näiteks samade kvaasiidentifikaatorite) alusel kokku viia. Sellisel juhul võib kahe andmestiku ühendamisel ilmneda, et neis kummaski esineb sarnane kordumatu kvaasiidentifikaatorite kombinatsioon, mis võimaldab mõne isiku kohta saada lisateavet ja teda tuvastada. Andmestike ühendamine ongi olnud peamine viis, kuidas algul anonüümseks peetavate andmete põhjal on siiski suudetud isikuid tuvastada.

Loe lisaks

- Genealoogiliste andmebaaside ja anonüümsete DNA doonorite andmete ühendamine: Bohannon, J. (2013). Genealogy Databases Enable Naming of Anonymous DNA Donors. Science, 339(6117), 262
- Netflixi kasutajate tuvastamine anonüümseks peetud filmireitingute andmete põhjal: Narayanan, A.; Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. IEEE Symposium on Security and Privacy, 111–125

- **Järeldamine** (*inference*) on võimalik juhul, kui andmestikus esineva isiku kohta on teada lisainfot. Näiteks koos töötavad või õppivad inimesed teavad oma kaaslaste kohta rohkem ja võivad ka otseste identifikaatoriteta andmestikest üksteist ära tunda. Lisainfoks võib olla ka lihtsalt teadmine, et keegi tuttav osales uuringus – järelikult käib üks andmestikurida tema kohta. Samuti võib inimese ära tunda hääle või isikupärase sõnakasutuse järgi. Järeldamise erijuht on see, kui inimene ise ennast andmestikust ära tunneb.

  Järeldamist on küllaltki keeruline vältida, kuna võimalike taustateadmiste hulk on määramatu ja sõltub konkreetsest isikust. Samuti tuleks arvestada, et *k*-anonüümsus ei pruugi järeldamise teel saadud teadmiste eest kaitsta, kui kaitstavad tunnused on ühetaolised.

  Näide

  Andmestikus esineb vähemalt viis (*k* = 5) vastet kombinatsioonile, mis koosneb neljast tunnusest: naine, 30–40-aastane, pärit Tartust, töösuhe: lapsehoolduspuhkusel. Piisab vaid kolme tunnuse teadmisest, et saada neljanda tunnuse kohta lisateavet või isik tuvastada. Sellisel juhul tuleks kaaluda ***l*-hajutuse** (*l-diversity*) näitajat, mis eeldab, et ka iga tundliku tunnuse kohta esineb eri väärtuseid. Näiteks *l*-hajutus = 2 eeldaks, et nende viie 30–40aastase Tartust pärit naise puhul peaks töösuhtel olema vähemalt kaks väärtust: mõni neist *lapsehoolduspuhkusel*, mõni *aktiivse töösuhtega*, *töötu* vms.

- **Tehnoloogia arengu või uute andmestikega ühendamise tõttu** võib anonüümitud isikute tuvastamine muutuda mingil hetkel võimalikuks, eriti kui andmeid säilitatakse aastakümneid. Sel juhul tuleb hinnata tuvastamisriski ja võtta arvesse, et kui andmed muutuvad tuvastatavaks, rakenduvad uuesti andmekaitsepõhimõtted. Vastutav töötleja peab sel juhul hindama mõistlikul määral tuvastatavust ja tõendama, et andmeid võib tõesti anonüümseks pidada.

3.4.5. Kuidas teha anonüümset küsitlust?

Anonüümse küsitluse käigus kogutakse vastuseid sellisel kujul ja viisil, et vastajaid ei ole võimalik kuidagi tuvastada.

Kui inimestelt kogutakse andmeid veebiküsitluses, tuleb arvestada, et ka IP-aadressid on isikuandmed (vt ka p 1.3.2) ja nende salvestumisel võivad isikud olla tuvastatavad. Sel juhul ei ole küsitlus anonüümne, vaid selle käigus kogutakse isikuandmeid. Anonüümimine on siiski võimalik, kui andmeid järeltöödelda – näiteks kustutada IP-aadressid pärast andmekogumist jäädavalt. Küsitluses osalejatele tuleb nii isikuandmete kogumisest kui ka nende hilisemast anonüümimisest selgelt teada anda.

Mõni küsitluskeskkond võimaldab andmete kogumisel seadistada ka seda, milliseid lisaandmeid küsitluses salvestatakse. Kui IP-aadresside ja muude andmete kogumine on võimalik välja lülitada, võib andmete kogumist pidada anonüümseks. Siiski peab arvestama võimalusega, et ka väga hoolikalt seadistatud küsitluse vastused võivad muuta inimese tuvastatavaks – piisab, kui paluda näiteks inimese kontaktandmeid.

Ülikoolis on soovitatav kasutada küsitluskeskkonda LimeSurvey, mis pakub anonüümsuse tagamiseks lisavalikuid, sh vastaja IP-aadressi automaatse salvestamise väljalülitamist. Kui teadlane kasutab LimeSurveyd või muud ülikoolis tunnustatud keskkonda, saab ta küsimuste korral tuge arvutiabilt (arvutiabi@ut.ee). Ülikoolivälistes keskkondades ei ole arvutiabil teadlast probleemide tekkimisel võimalik aidata.

3.5. Mida teha andmekaitsealase rikkumise korral?

Isikuandmetega seotud rikkumine on üldmääruse artikli 4 punkti 12 kohaselt turvanõuete eiramine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu.

Andmekaitsealase rikkumisega on tegemist näiteks siis, kui

- avalikuks on saanud andmed, mis ei tohiks olla avalikud;
- andmed on kogemata kustutatud või neile ei saa vajalike toimingute tegemiseks enam juurdepääsu ka mitte varukoopia taastamisel;
- andmetele on pääsenud juurde volitamata isikud: näiteks kaasatakse teadusuuringu andmeanalüüsi etappi üliõpilasi, aga nendega ei sõlmita enne konfidentsiaalsuslepet;
- teadusuuringu jaoks on küsitud kirjalik nõusolek kindlal eesmärgil andmete töötlemiseks, aga neid andmeid kasutatakse uuringuga mitte seotud eesmärgil;
- isikuandmeid kogutakse vaikimisi nõusoleku (*opt-out*) alusel, millest keeldumiseks peab andmesubjekt astuma samme.

Rikkumine võib kahjustada inimest ja tema huve, põhjustades füüsilist, materiaalset või mittemateriaalset kahju. Selle vältimiseks on ülikoolil kui vastutaval töötlejal kohustus saada täielik ülevaade andmete töötlemisest ja kontroll selle üle.

3.5.1. Andmekaitsealasest rikkumisest tuleb kohe teada anda

Kui ülikoolis toimub isikuandmete alane rikkumine, tuleb sellest viivitamata teavitada ülikooli andmekaitse peaspetsialisti (andmekaitse@ut.ee). Tegutseda tuleb võimalikult kiiresti, et lõpetada näiteks volitamata juurdepääs andmetele, nende väärkasutus või muu rikkumine. Et hoida ära sarnased juhtumid tulevikus, võib olla vajalik anda juhtumist teada ka arvutiabile (arvutiabi@ut.ee).

Andmekaitse peaspetsialisti tuleb teavitada ka juhul, kui on vaid rikkumise kahtlus – siis saab täpsemad asjaolud välja selgitada.

3.5.2. Pärast rikkumisest teavitamist tuleb olla valmis teabe jagamiseks

Üldmääruse artikli 33 lõike 5 alusel on ülikoolil kohustus dokumenteerida kõik isikuandmetega seotud rikkumised, sealhulgas nende asjaolud, mõju ja võetud parandusmeetmed. Seepärast hakatakse pärast rikkumist seda uurima ja vajaduse korral lisateavet koguma. Rikkumisega seotud inimestel tuleb olla valmis andma andmekaitsespetsialistile kirjalikke selgitusi või esitama vajalikke materjale.

Rikkumise põhjuste ja tagajärgedega tegelemiseks tuleb varuda aega. On väga oluline tekkinud olukord lahendada (andmeleke lõpetada, andmesubjekte teavitada, hinnata, mis juhtus ja miks, teha kindlaks, kui paljudele andmed avaldati, kogu protsess üle vaadata jm). See kõik on väga ajamahukas.

Ülikooli andmekaitse peaspetsialist teavitab rikkumisest ka Andmekaitse Inspektsiooni, kes võib omakorda ülikooli suhtes rikkumismenetlust alustada.

3.5.3. Rikkumise võimalikud tagajärjed

Kui rikkumise uurimine on lõppenud, tuleb leida lahendused, mis tagavad, et samasugust intsidenti enam ei juhtu. Näiteks võib rakendada lisakaitsemeetmeid, suurendada teadlikkust, korrigeerida protseduure vms.

Üldmääruse artikli 82 lõike 1 järgi on igaühel, kes on isikuandmete alase rikkumise tõttu kannatanud materiaalset või mittemateriaalset kahju, õigus saada vastutavalt või volitatud töötlejalt hüvitist tekitatud kahju eest. IKS-i 6. peatükis loetletakse vastutava töötleja kohustuste rikkumisel kohaldatavate rahatrahvide suurus. Andmekaitse Inspektsioon võib ettekirjutuse täitmatajätmise korral rakendada sunniraha. Samuti võib ülikool võtta töötaja vastutusele, kui selgub, et rikkumine on toimunud tema hooletuse tõttu.

Lisaks IKS-ile ja üldmäärusele on isikuandmete alaste rikkumiste eest sätestatud sanktsioonid ka karistusseadustiku §-des 157–157[2]. Karistusseadustik võimaldab vastutusele võtta süüteo toime pannud füüsilist isikut ehk konkreetset ülikooli töötajat, kelle süül rikkumine toimus.

Loe lisaks

- Ülikoolis rikkumise korral järgitavad juhised
- Ülikooli küberturbe juhised
- Ülikooli asjaajamiseeskirja peatüki IX punktid 55–57, mis puudutavad käitumist rikkumise korral

3.6. Mida teha, kui andmesubjektilt tuleb päring oma andmete kohta?

Kui inimene pöördub teadlase või ülikooli poole päringuga, mis puudutab tema andmete töötlemist, tuleb sellele 30 päeva jooksul vastata.

- **Pöördumine** tuleb dokumenteerida. Tartu Ülikooli kui vastutava töötleja peamine dokumenteerimisvahend on dokumendihaldussüsteem, kuhu päringu saaja peab päringu üles laadima. Dokumenteerimise alusel saab määrata vastamistähtaja, mis võimaldab kontrollida, kas igale päringule on vastatud. Kasutada võib ka muid dokumenteerimissüsteeme, mis aitavad ülikoolil saabunud päringutel ja neile vastamisel silma peal hoida, kuid dokumendihaldussüsteemis peab päring ikkagi registreeritud olema.

- **Andmesubjekt tuleb tuvastada.** Kuna isikuandmeid ei tohi anda kolmandatele isikutele, tuleb kindlaks teha, et pöörduja on sama andmesubjekt, kelle andmete kohta infot soovitakse. Et infootsija tuvastada, tuleb paluda enne andmete andmist esitada taotlus digitaalselt allkirjastatuna.
- **Enne vastamist tuleb kindlaks teha päringule vastamise teostatavus.** Pöördumise aluseks peab olema mõni andmesubjekti õigus (vt alaptk 2.9). Kui soovitakse näiteks ülevaadet teadustöös töödeldavatest isikuandmetest, tuleb see kindlasti küsijale anda. Osa õigustest – näiteks õigus esitada vastuväiteid – kehtib vaid erijuhtudel, mille kohta võib küsida abi andmekaitsespetsialistilt. Kui päring sisaldab palvet kustutada andmed, tuleb teostatavuse kindlakstegemisel arvestada ka võimalusega, et isikuandmed sisalduvad varukoopiates, kust võib olla keeruline andmeid kustutada.

  Kõige keerulisem päring puudutab õigust oma andmetega tutvuda. Ülikoolil on kohustus täita mõistlikke päringuid, st ükski andmesubjekti õigus ei ole absoluutne. Kui päringule vastamine pole teostatav, tuleb selgitada selle põhjust (vt ka p 2.9.2).

Sõltumata sellest, kas andmesubjekti päringule vastamine on teostatav või mitte, tuleb talle igal juhul tähtaja jooksul vastata. Ühtset vastusevormi ega vastamisprotseduuri ei ole kehtestatud, nii et vastuse vormistus sõltub enamasti küsimusest.

Andmesubjekti päringut saades tasub pidada nõu andmekaitse peaspetsialistiga, kellele saab kirjutada e-posti aadressil andmekaitse@ut.ee.

4. Teadustöö tulemuste avaldamine ja andmete säilitamine

Andmekaitse on oluline ka pärast teadustöö lõppu. Peale andmekaitsepõhimõtete jätkuva järgimise tuleb teada, kuidas andmeid avaldada ja säilitada. Selles peatükis on käsitletud peamisi küsimusi, mis võivad isikuandmete jagamisel tekkida, ja antud mõningaid soovitusi.

Avaliku huvi seisukohast on olulised nii teadustöö vahetu tulemus kui ka selle ühiskondlik levik ja kasutus. Ka avatud teaduse eesmärkide saavutamine eeldab, et teadustöö tulemused ja nende saamiseks kasutatud andmed oleksid püsivalt ja pikka aega kättesaadavad kõigile huvilistele. Euroopa Liidu avaandmete direktiivi 2019/1024 artikli 10 lg-s 1 on sätestatud: „Liikmesriigid toetavad teadusandmete kättesaadavust ning kehtestavad selleks riigisisesed põhimõtted ja asjaomased meetmed, et muuta avaliku sektori rahastatud teadusandmed vaikimisi avatuse põhimõtet järgides vabalt kättesaadavaks („vaba juurdepääsu põhimõte“) ja FAIR-põhimõtetega ühilduvaks.“

Loe lisaks

Tartu Ülikooli raamatukogu andmehaldusplaani koostamise juhendi peatükk „Andmete pikaajaline säilitamine“

4.1. Kui kaua võib teadustöös kasutatud isikuandmeid säilitada?

Isikuandmete säilitamisel lahknevad andmekaitse ja avatud teaduse põhimõtted mõnevõrra. Minimaalsus- ja säilitamispiirangu põhimõte eeldavad, et isikuandmeid tuleb töödelda nii lühikest aega kui võimalik ning pärast eesmärkide täitmist tuleks andmed kustutada või anonüümida. Kuid avatud teaduse huvides on tagada juurdepääs teadusandmetele võimalikult kaua, vähemalt seni, kuni need on teadlastele või ühiskonnale väärtuslikud. Kuna teaduse seisukohast on oluline uurida ka ajaloolisi sündmusi ja arengusuundmusi, võrrelda varasemaid nähtusi tänapäevastega või mõista üldisemalt protsesside kulgu, siis ei saa määrata ühest tähtaega, misjärel andmed oma teadusliku väärtuse kaotavad.

Üldmääruse artikli 5 lg 1 p e kohaselt võib isikuandmeid isikustatud kujul säilitada esialgse eesmärgi täitmisest kauem, kui seda tehakse üksnes teadusuuringute eesmärgil ja sealjuures rakendatakse tehnilisi ja korralduslikke meetmeid inimeste eraelu kaitsmiseks. Seega pakub üldmäärus teadustööga seotud isikuandmete säilitamisel suuremat paindlikkust. Samas rõhutab Euroopa Andmekaitseinspektor esialgses arvamuses andmekaitse ja teadusuuringute kohta (lk 18), et seda erandit ei tohi kasutada viisil, mis õõnestaks andmekaitse üldisi eesmärke. Näiteks kuritarvitatakse teadustööga kaasnevaid privileege, kui isikuandmeid säilitatakse tähtajatult (säilitamispiirangu erand) ja samal ajal piiratakse isikute õigusi enda teabe suhtes (andmesubjektide õiguste erandid). Teadustööga seotud erandile saab seepärast toetuda vaid juhul, kui isikuandmete jätkuv säilitamine on õiguspärane, vajalik ja proportsionaalne.

Et isikuandmeid saaks algse eesmärgi täitmisest kauem säilitada, tuleb seega täita järgmisi tingimusi.

- **Üksnes teadustöö eesmärgil**: erandi andmisel on silmas peetud vaid teadustöö vajadusi ning seda ei tohiks kasutada isikuandmete piiramatuks säilitamiseks muudel eesmärkidel, mis on eraviisilist või ärilist laadi. Erand on tehtud ka avalikes huvides toimuva arhiveerimise ning statistika korral, mistõttu võib kauem säilitada ka isikuandmeid, mis on arhiiviväärtuslikud või

olulised statistika tegemiseks. Selge piiri tõmbamine teaduse, arhiveerimise ja statistika vahele ei ole alati lihtne, nii et teadustööd võivad puudutada mõlemad erandid.

- **Tehnilised ja korralduslikud meetmed:** pikem säilitamine eeldab isikuandmete turvalist talletamist. Kui teadusuuringu tegemise ajal on oluline andmete käideldavus, siis säilitamise ajal väheneb käideldavuse olulisus ja kaaluda võib turvalisemaid talletamislahendusi. Näiteks võib piirata töörühma liikmete ligipääsu isikuandmetele.

- **Kaaluma peaks andmete anonüümimist**. Anonüümitud andmeid võib säilitada tähtajatult ja jagada ka avaandmete repositooriumis. Säilitamise eesmärgil anonüümimine tuleks siiski juba varakult kokku leppida ja see kavatsus tuleb selgelt kirja panna nii andmehaldusplaani kui ka teadusuuringus osalejatele antavasse teabesse. Kui anonüümine pole võimalik, tuleks isikuandmed pseudonüümida, aga sellisel juhul kohaldub sellele üldmäärus.

- **Säilitama peaks vaid väärtuslikud andmed**. Andmete säilitamisel tuleb järgida minimaalsuspõhimõtet, st alles tuleb jätta vaid kõige olulisemad andmed, mille pikaaegne hoidmine isikustatud kujul on vajalik ja põhjendatud. Kuna teadustöö suhtes kohalduv erand eeldab niikuinii eri huvide ja vajaduste tasakaalustamist, võib abiks olla see, kui piiritleda andmestiku sees säilitamist vajavad andmed, mis on kas suure pikaaegse teadusliku väärtusega või vajalikud tulemuste valideerimiseks. Igaks juhuks säilitamine ei ole üldmääruse kohaselt lubatud.

- **Säilitamine peab olema läbipaistev ja õiglane**. Isikuandmete säilitamise erandile toetumine peaks olema teada juba teadusuuringut kavandades. Läbipaistev ja õiglane ei ole see, kui alles teadusuuringu lõppedes otsustatakse teadusrühmas teatud isikuandmeid kauem säilitada. Kinni tuleb pidada ka andmesubjektile antud lubadustest: kui talle on öeldud, et andmed pärast uuringu lõppu hävitatakse, ei ole lubatud neid alles hoida. Keeruline on olukord siis, kui teadustöö tegemise käigus selgub, et kogutud andmed on oodatust palju väärtuslikumad, kuid plaanitud on kõik andmed hävitada. Isikuandmete edasine kasutus uutes teadusuuringutes ning pikem säilitamine on üldmääruse kohaselt küll võimalik, kuid algse otsuse muutmine peab olema inimeste jaoks õiglane ja läbipaistev.

- **Võimaluse korral tuleks käsitada isikuandmete säilitamist eraldi eesmärgina.** Sel juhul tuleb leida uuele eesmärgile sobiv õiguslik alus.

4.2. Millisel kujul võib isikuandmeid avaldada?

Avaldamist mõistetakse kui isikuandmetele juurdepääsu võimaldamist piiramatule inimeste ringile kas avalikul veebilehel, avalikus andmebaasis või muus kohas. Avaldamine on võimalik vaid juhul, kui andmete konfidentsiaalsust ei pea tagama. Kuna üldjuhul eeldab turvalisuspõhimõte, et kaitsta tuleb ka isikuandmete konfidentsiaalsust, on isikustatud andmete avaldamise kohta tehtud teadustöö puhul erand.

Andmete avalikustamine ei puuduta olukordi, kui inimene soovib enda andmetest koopiat või kui andmeid jagatakse teadusasutuste vahel.

4.2.1. Andmete avaldamine isikustatud kujul

Kuna isikustatud andmete avaldamine ei ole enamasti uurimistöö puhul vajalik, tuleks seda käsitada eraldi eesmärgina, mis vajab ka iseseisvat, üheselt mõistetavat ja selget õiguslikku alust. Teadustöö puhul sobib selleks eraldi andmesubjekti nõusolek. Kui avaldamine ei põhine nõusolekul, tuleb järgida IKS-i § 6 nõudeid.

Mõningate isikustatud andmete avaldamine võib olla vajalik ka juhul, kui teadustöös on uuritud inimeste loomingut, näiteks kirjalikus või suulises vormis teoseid (jutustused, elulood, meedias avaldatud tekstid jms). Sellisel juhul võib uuritud tekstide ja muude teoste autorite nimede avaldamine olla vajalik ja põhjendatud. Teoste autorite nimetamine ja neile viitamine ilma nõusolekuta on lubatud akadeemilise, kunstilise ja kirjandusliku eneseväljenduse eesmärgil (vt IKS-i § 5).

4.2.2. Andmete avaldamine pseudonüümitud kujul

Kuna pseudonüümitud andmed on isikuandmed, peab nende avaldamine põhinema selgel õiguslikul alusel ja olema kooskõlas andmete töötlemise eesmärgiga. Pseudonüümimine pakub vaid lisakaitset inimeste tuvastamise vastu, kuid ei anna iseenesest õigust andmete avaldamiseks.

Pseudonüümitud andmete avaldamiseks võib pidada näiteks seda, kui tsiteeritakse lauseid avaldamata tekstidest (nt intervjuu transkriptsioon) ja neile viidatakse pseudonüümi või isikustamist välistava fraasiga (nt „… intervjuus osalenud doktorandi sõnul …“). Kui aga tsiteeritakse avalikustatud tekste (nt sotsiaalmeedia kommentaarid), peab arvestama, et nende autorid võivad olla lihtsasti tuvastatavad.

Teadlane peab täitma uuringus osalejatele antud lubadusi. Kui ta lubab anonüümsust, on keelatud pseudonüümitud andmeid avaldada. Kui ta aga lubab, et uuringus osalejate nimesid ja isikustamist võimaldavaid andmeid hoitakse konfidentsiaalsena, võib pseudonüümitud andmeid avaldada, kui see on teadustöö eesmärgil vajalik. Eesmärgipärane ei ole näiteks see, kui teadlane avaldab enda jaoks huvitavaid või kummalisi pseudonüümitud intervjuukatkeid isiklikus sotsiaalmeediakanalis – selline töötlemine väljub teadustöö piirest ja on vastuolus andmesubjekti ootustega.

Pseudonüümitud kujul võib kogu andmestiku avaldada, kui selleks esineb õiguslik alus, järgitud on andmekaitsepõhimõtteid ja andmestiku anonüümimine ei ole võimalik. Ent sellisel juhul vastutab ülikool avalikustamisega põhjustatud tagajärgede eest.

4.2.3. Andmete avaldamine anonüümitud kujul

Eelistatuim on avalikustada ja jagada anonüümitud andmeid, sest need ei ole enam isikuandmed ja seetõttu ei kehti nende kasutamisele ühtki lisapiirangut. Üldmäärus ja avaandmete direktiiv (EL) 2019/1024 soosivad teadusandmete kättesaadavust ja laialdast kasutust ning lihtsaim viis seda tagada on anonüümida isikuandmeid sisaldavad teadustööd.

4.3. Kellega võib teadustööd tehes isikuandmeid jagada?

Isikuandmeid saab jagada kas andmetest koopia edastamise või neile juurdepääsu võimaldamise teel. Mõlemal juhul tuleb hinnata, kas vastutaval töötlejal on õigus isikuandmeid jagada. Allpool on esitatud tüüpilisemad andmete jagamise juhud.

4.3.1. Andmete töötlemine uurimisrühmas

Kui ülikooli ehk vastutava töötleja esindajad töötlevad töösuhte alusel isikuandmeid, ei kehti sellisele töötlemisele üldmääruse kohaselt lisapiiranguid. Siiski peab silmas pidama üldpõhimõtteid, nagu eesmärgipärasus, minimaalsus ja turvalisus (vt alaptk 1.5), mille alusel ei tohi isikuandmeid jagada ülikooli iga töötajaga. Seega tuleb iga üksiku teadlase vajadus isikuandmeid töödelda uurimisrühmas või ülikoolis kokku leppida. Näiteks saab andmehaldusplaanis nimetada teadlased, kellel on juurdepääs isikustatud kujul andmetele, kes pseudonüümivad, kes hoiavad pseudonüümimise saladust ja kes töötlevad vaid pseudonüümitud andmeid. Andmeid võib seejärel jagada vaid teadlastega, kes on andmehaldusplaanis nimetatud.

Kõigil uurimisrühma liikmetel ei pruugi olla ülikooliga töölepingut. Sel juhul tuleb neile anda volitus isikuandmete töötlemiseks.

4.3.2. Andmete töötlemine mitme teadusasutuse koostöös

Suuremate projektide puhul võib vastutus isikuandmete eest jaguneda eri teadusasutuste vahel ja sel juhul tuleb tähelepanu pöörata nende rollile ja kohustustele. Üldiselt tuleks teadusasutuste vahelistes lepingutes määrata selgelt kindlaks andmekaitsealase vastutuse jaotus ja see, kuidas isikuandmeid omavahel jagatakse. Järgida tuleb andmekaitsepõhimõtteid, mille kohaselt ei ole isikustatud andmed juurdepääsetavad kõigile projekti partneritele, vaid ainult neile, kelle ülesanne on neid töödelda. Partnerite vahel tuleks andmeid jagada võimaluse korral vaid pseudonüümitud kujul ja turvalisi lahendusi kasutades.

4.3.3. Andmete töötlemine juhendaja ja juhendatava koostöös

Ülikooli piires toimuva juhendamise korral ei ole isikuandmete jagamisel otseselt piiranguid, kuna nii juhendaja kui ka juhendatav on vastutava töötleja ehk ülikooli esindajad. Nende koostöö ja andmete jagamine peab olema läbipaistev: kui isikustatud andmeid näeb ka juhendaja, ei saa andmesubjektidele lubada, et keegi peale juhendatava isikuandmeid ei töötle.

4.3.4. Andmete jagamine teiste teadlaste, kirjastuste, repositooriumide või avalikkusega

Isikuandmete jagamiseks laiemas ringis on eelistatuim lahendus need eelnevalt anonüümida. Kui see ei ole miskipärast võimalik, eeldab isikuandmete edastamine kolmandatele isikutele õiguslikku alust – ilma selleta isikuandmeid jagada ei või. Lisaks võib kaaluda uuritavatelt laia nõusoleku küsimist selle kohta, et näiteks pseudonüümitud andmeid võib säilitada ja jagada võimalike tulevaste uuringute tarbeks. Kui jagada IKS-i § 6 alusel isikuandmeid ilma nõusolekuta, tuleks seda teha pseudonüümitud kujul.

Veel tuleb veenduda, et isikuandmete vastuvõtja tagab nende piisava kaitse. Selleks võib sõlmida temaga eraldi lepingu, kus lepitakse kokku isikuandmete kasutamise tingimused, sealhulgas see, kuidas jaguneb vastutus poolte vahel, kes pääsevad andmetele juurde. Näiteks on võimalik paigutada isikuandmed talletamiseks avaandmete repositooriumi, kuid piirata neile juurdepääsu ja tagada seeläbi nende konfidentsiaalsus. Enne repositooriumi kasutamist tuleks veenduda, et sellel on olemas andmekaitsetingimused, mis on kirjas teenuse kasutustingimustes või eraldi dokumendina. Paljud teaduskirjastused paluvad autoritel esitada ka andmete kättesaadavuse avaldus (vt p 4.3.5).

Ehkki isikuandmete lubamatu jagamise eest vastutab seda teinud teadlane, laieneb see vastutus paratamatult ka ülikoolile vastutava töötlejana, kes peab fikseerima andmekaitsealase rikkumise ja sellest teada andma (vt alaptk 3.5).

4.3.5. Andmete jagamise tingimused kirjastustes

Avatud teaduse üks eeldus on see, et teadusuuringus kasutatud andmetele pääsevad juurde kõik teised teadlased kas varasemate uuringute kontrollimiseks või täiesti uuteks uuringuteks. Sel eesmärgil on paljudes kirjastustes kehtestatud andmejagamispõhimõtted, millega nõustumisel eeldatakse artiklite autoritelt andmete jagamist teiste teadlastega.

Uueks tavaks on kujunenud kirjastajate nõue, et teadustekstide publitseerimisel tuleb teadlastel täita **andmete kättesaadavuse avaldus**, milles tuleb kirjeldada, kas, kus ja kuidas on teadusandmed kättesaadavad teistele teadlastele. Avaldusse saab lisada kolm isikuandmete kasutamise võimalust:

- **kui andmed on juba avalikud**, tuleks avalduses viidata, kus need asuvad, olgu selleks teadusandmete repositoorium või mõni muu avaandmete keskkond;
- **kui andmeid tuleb autoritelt küsida**, pannakse avaldusse kirja, et neid jagatakse vaid päringu esitamisel. Samuti on võimalik seada lisatingimusi, näiteks et päringu saab esitada vaid doktorikraadiga teadlane või uuringu põhitäitja. Sellised tingimused eeldavad, et esineb mõjuv põhjus, miks andmeid ei saa lihtsalt avaldada. Andmeid küsiva teadlasega sõlmitakse enne andmete üleandmist konfidentsiaalsusleping;
- **kui andmeid ei saa jagada**, tuleb avalduses põhjendada, miks see ei ole võimalik ega lubatud. Üks põhjus võib olla vajadus kaitsta inimeste eraelu.