



## ISIKUANDMETE TÖÖTLEMINE ANDMEANALÜÜTIKAS

29. aprill 2022  
vandeadvokaat Margot Arnus



Koolituse „Isikuandmete töötlemine andmeanalüütikas“ materjalid. Koolitus toimus 29.04.2022.



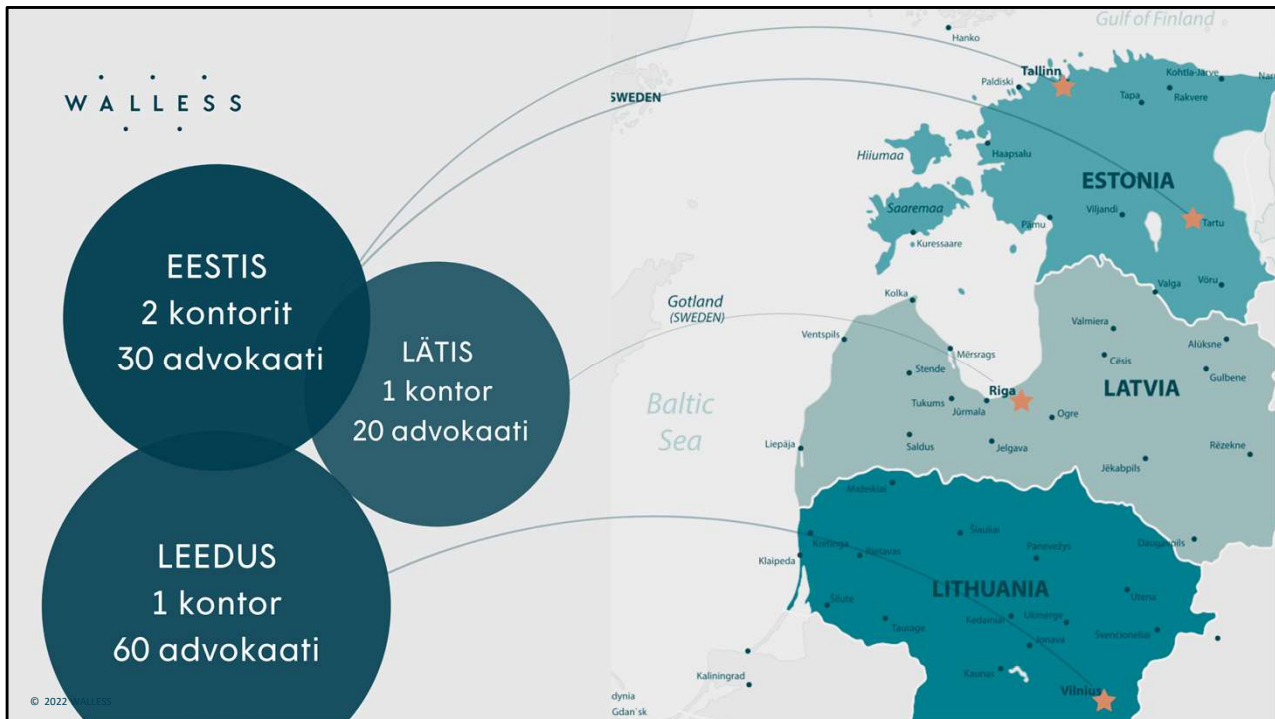
## MARGOT ARNUS

andmekaitseametnik, vandeadvokaat

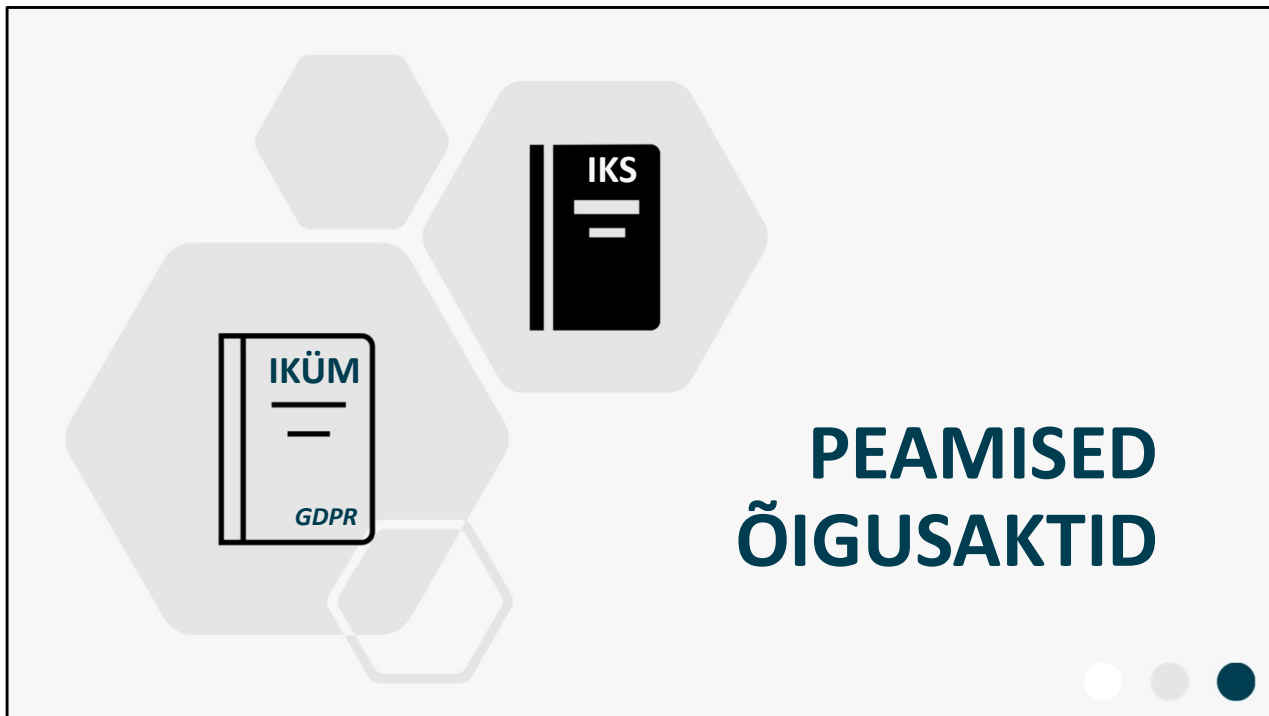
Telefon: +372 53 44 03 24

E-post: [margot.arnus@walless.com](mailto:margot.arnus@walless.com)

Advokaadibüroo WALLESS vandeadvokaat Margot Arnus on spetsialiseerunud andmekaitse ja IT-õigusega seonduvate küsimuste lahendamisele ning lepinguõigusele. Lisaks igapäevasele advokaaditööle on Margot külalislektorina andnud intellektuaalomandi teemadel loenguid ka TalTechis.



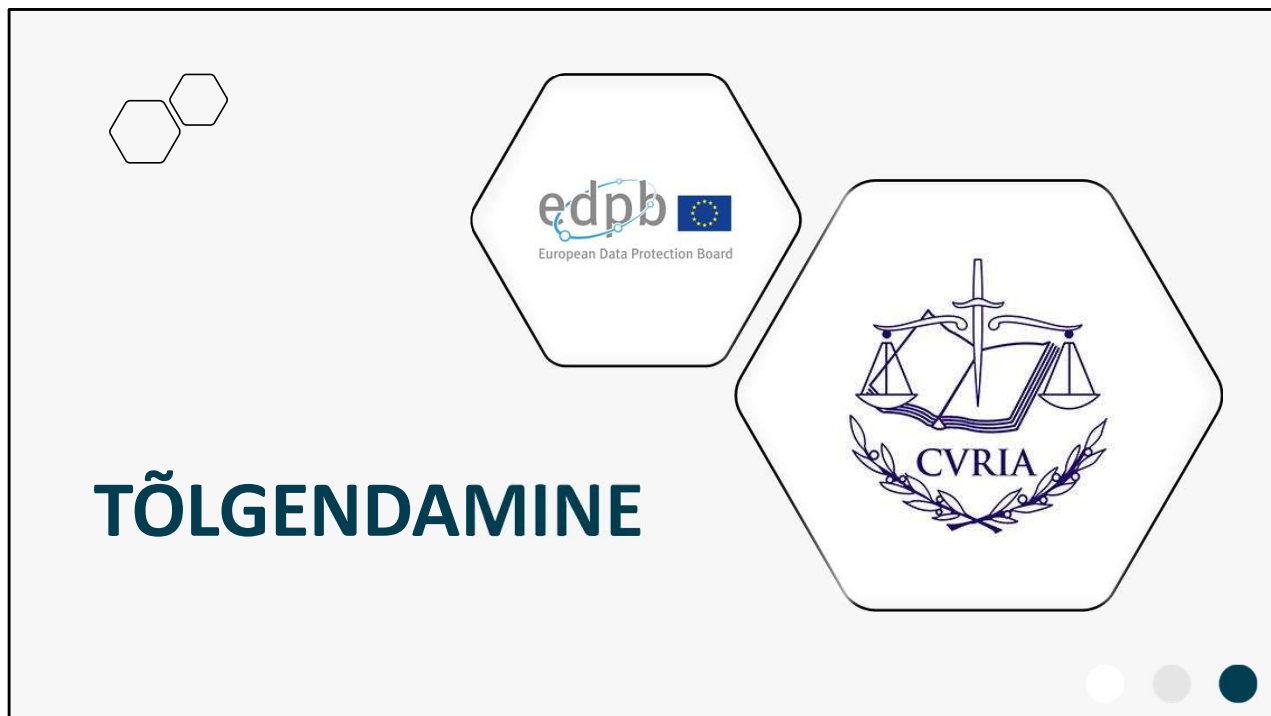
WALLESSil on kontorid nii Eestis, Lätis kui ka Leedus. WALLESSi edu alus on veendumus, et kaasaegse advokaadibüroo ärimudel põhineb avatusel ja läbipaistvusel. WALLESSi võimekas advokaatide meeskond seab klientide vajadused esiplaanile ja leiab neile sobivad uuendusmeelsed juriidilised lahendused. Loo me pidevalt oma klientidele teedrajavaid sektoripõhiseid lahendusi. Rohkem saate büroo ja ka meie tegevusvaldkondade kohta lugeda kodulehelt: <https://walless.com/et/>.



**Isikuandmete kaitse üldmäärus:** Euroopa Parlamendi ja Nõukogu 27. aprilli 2016 määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta.

**Isikuandmete kaitse seadus** (RT I, 04.01.2019, 11): Sätestab osaliselt IKÜM-ist tulenevad erisused, kuid peamiselt on selle aluseks õiguskaitseasutuste direktiiv. NB! IKS-is ca 10 üldiselt kohalduvat paragrahvi, edasi kogu ptk 4. on isikuandmete töötlemine õiguskaitseasutuse poolt. Koolitus keskendub üldisemalt IKÜM-ile.

**Õiguskaitseasutuste direktiiv:** Euroopa Parlamendi ja Nõukogu 27. aprill 2016 direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK.



Isikuandmete kaitse üldmäärust aitavad tõlgendada õiguskirjadus ja kohtupraktika. Kohtupraktikat on esialgu veel väga vähe, sest tegemist on suhteliselt värskest jõustunud õigusaktiga. Siiski kujunevad tasapisi juba nii mõnedki seisukohad ka kohtupraktika pinnalt, sh korratakse üle enne IKÜM-i jõustumist kehtinud põhjendusi ja tõlgendusi.

**Euroopa Andmekaitseõukogu** on sõltumatu Euroopa asutus, mis tagab andmekaitsereeglite ühtse kohaldamise kõikjal Euroopa Liidus ning edendab koostööd ELi andmekaitseasutuste vahel. See asendas IKÜM jõustumisel 2018. aasta mais nn artikli 29 tööühma.

Andmekaitseõukogu eesmärk on tagada kogu Euroopa Liidus isikuandmetekaitse üldmääruse ja Euroopa õiguskaitse direktiivi ühtne kohaldamine. Selleks väljastab Andmekaitseõukogu üldisi suuniseid, sealhulgas suuniseid, soovitusi ja parimaid tavasid, et selgitada andmekaitseõiguse sätteid. Samuti nõustab Andmekaitseõukogu Euroopa Komisjoni mis tahes isikuandmete kaitse küsimuses ja uute Euroopa Liidus kavandatavate õigusaktide teemal. Andmekaitseõukogu võtab vastu ka ühtseid järeldusi piiriüleste andmekaitsejuhtumite kohta ning edendab koostööd ja tõhusat teabevahetust, samuti parimate tavade jagamist, riiklike järelevalveasutuste vahel.

Rohkem infot: [https://edpb.europa.eu/about-edpb/about-edpb/who-we-are\\_et](https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_et)

# MIS ON ISIKUANDMED?

See võib tunduda lihtne küsimus, aga tegelikult on just sellel küsimusel kandev tähtsus andmekaitstes üldiselt ja kindlasti andmeanalüütikas. Sellest oleneb, mis mängureeglid kohalduvad.

Kuigi esialgu võib tunduda, et vastus on ilmselge, siis tegelikult on väga palju nüansse ja varjundeid. Nt kui küsida, kas NIMI on isikuandmed, siis ilmselt esimese hooga paljud vastavad JAH. Aga kui tegemist on sagedasti esineva nimega, ei võimalda ainult nimi isikut üheselt tuvastada.

<p><b>MÕISTE</b></p> <p><b>IKÜM artikkel 4 p 1</b></p>	<p><b>„Isikuandmed“ on ...</b></p> <ul style="list-style-type: none"><li>... igasugune teave ...</li><li>... tuvastatud või tuvastatava</li><li>... füüsilise isiku („andmesubjekti“) kohta.</li></ul> <p>Tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.</p>
--	--

IKÜM artikkel 4 p 1 definitsioon isikuandmete kohta.

# MILLAL ON ANDMESUBJEKT TUVASTATAV?

Õigusakte lugedes sageli esmapilgul kõik sõnad tuttavad ja mõte selge, aga kui süveneda, siis tõlgendus palju keerukam. Näiteks, mida tähendab, et andmesubjekt on „tuvastatav“?



<b>MÕISTE</b>	<b>Tuvastatav füüsiline isik</b> on isik, keda saab ...
<b>IKÜM artikkel 4 p 1</b>	... otseselt või kaudselt tuvastada, ...
	... eelkõige sellise identifitseerimistunnuse põhjal nagu ...
	... nimi, isikukood, asukohateave, võrguidentifikaator või ...
	... selle füüsilise isiku <b>ühe või mitme</b> füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.

Isegi kui andmekategooria üldjuhul viitab isikuandmetele, ei pruugi ainult üks andmepunkt isiku tuvastamist võimaldada. Näiteks aadressi peetakse üldjuhul isikuandmeteks, kuid kahe või rohkema pereliikmega korteri puhul on nende identifitseerimiseks vaja teada vähemalt ühte täiendavat (eristavat) tunnust.

Isikut on võimalik tuvastada isegi juhul, kui ei ole teada isiku nime, isikukoodi jne. Määrav on, et andmekogum on piisavalt spetsiifiline, et need andmepunktid käivad ainult ühe konkreetse isiku kohta. Kui tabelis pikkus ja kaal, siis isegi kui mul on sama pikkus ja kaal, ei käi need andmed minu kohta. Kui on aga pikkus, kaal, sugu, vanus, juukse- ja silmavärv ja mõni asjakohane punkt veel, siis ei pruugi leiduda teist samade parameetritega isikut, st on tegemist isikuandmetega.

**SELGITUS**

**IKÜM põhjendus p 26**

Tuleb arvesse võtta **kõiki vahendeid**, mida mõistliku tõenäosusega võidakse tuvastamiseks kasutada.

Tuleb arvestada kõiki objektiivseid tegureid, näiteks tuvastamise **maksumus** ja selleks vajalik **aeg**, võttes arvesse nii andmete töötlemise ajal kättesaadavat tehnoloogiat kui ka tehnoloogilisi arenguid.

Nagu öeldud, „tuvastamine” ei tähenda üksnes võimalust leida isiku nimi ja/või aadress, vaid ka isikut eristada, seostada ja tuletada.

Lisaks ei ole andmekaitsealaste õigusaktide kohaldatavuse puhul oluline, millised on vastutava töötleja või vastuvõtja kavatsused. Andmekaitse-eeskirjad kehtivad seni, kuni andmed on tuvastatavad. Sh kui need on tuvastatavad teiste andmete (lihtsa) ühendamise kaudu.

Tasub silmas pidada ka kõiki pahatahtlike kavatsusi, ründevoimalusi jne.



Tegemist on hagejatega aset leidnud tõsieluliste sündmuste **ainetel loodud, mitte nende isikuandmetel põhineva teosega**. Mingi sündmuse ainetel teose loomist ei saa seostada üheselt isikuandmete kasutamisega ega isikuandmetel põhineva looga.

Identifitseerimata isiku kohta andmete kajastamisel ei saa järeltada konkreetse isiku eraeluliste andmete kajastamist.

Isik ei ole tuvastatav, kui tuvastamisele kulub ebamõistlikult aega, see on keerukas ja kulukas.

Tallinna Ringkonnakohtu 09.01.2019 otsus kohtuasjas nr 2-16-16730



Tallinna Ringkonnakohtu 09.01.2019. a otsuses kohtuasjas nr 2-16-16730 arutati elulistest sündmustest tuletatud teose (filmi) isikuandmeteks olemise teemal. Asjaoludega saab täpsemalt tutvuda otsust lugedes, kuid lühidalt räägib film „Sangarid“ neljast noorest spordipoisist, kes ajasid 80-ndatel Viru hotellis äri Soome turistidega. Aastal 1984 tärkas neil soov põgeneda Nõukogude Eestist paadiga Soome ja sealt edasi Rootsi. Nad said selleks kummipaadi ja põgenesid teatavate viperustega. Kohanemine Rootsi argieluga osutus keeruliseks, niisiis valiti otsetee suurema varani. Rööviti kullassepaäri ja ühe panga filiaali. Poisid saadi kätte (kuigi juveeliärist röövitud ehted ja kalliskivid on tänaseni kadunud) ja mõisteti mõneks ajaks vangi. Neli meest väitsid, et film kajastab nende elulugu ja nende isikuandmeid.

Filmi tegija väitis, et filmis esitatul puudub seos konkreetsete isikute ja sündmustega. Film on tehtud inspiratsioonina nendest sündmusest. See, kuidas hagejad püüavad meelevaldselt väita, et nende isikud on filmi tegelastega seostatavad läbi üksikute tunnuste nagu sugu, vanus, jõutreeningu tegemine, asukohariik vms, ei võimalda neid kogumis ega veel vähem üksikuna kuidagi mõistlikult identifitseerida. Mängufilmi puhul jälgitakse ja mõistetakse seda auditoriumi poolt ühe tervikliku loona. Seega ei piisa mängufilmi analüüsimisel ainult sellest, et jälgitakse vaid mingit konkreetset lõiku. Läbi isikuandmete väidetava kaitsmise püüavad hagejad teha nn "nende omaks" väga palju täiesti tavapäraseid olukordi.

Sellest saab tuua huvitava võrdluse sünteetiliste andmetega. Kuigi ka need on sageli loodud „päris“ andmestiku põhjal, siis sünteesi tulem ei ole enam isikuandmed..

TÄHTSUS

IKÜM põhjendus p 26

Andmekaitse põhimõtteid tuleks kohaldada tuvastatud või tuvastatavat füüsilist isikut puudutava igasuguse teabe suhtes.

Andmekaitse põhimõtteid **ei tuleks seetõttu kohaldada anonüümse teabe suhtes**, nimelt teave, mis ei ole seotud tuvastatud või tuvastatava füüsilise isikuga, või isikuandmete suhtes, mis on **muudetud anonüümseks** sellisel viisil, et andmesubjekti ei ole võimalik tuvastada või ei ole enam võimalik tuvastada.

Miks on oluline, kas on isikuandmed või mitte? Sellest olenevad kohaldatavad reeglid. Kui tegemist on tõesti täiesti anonüümsete andmetega, ei pea isikuandmete kaitse reegleid enam kohaldama. Küllaga tasub tähelepanelik olla, et suurt andmekogumit päriselt anonüümseks muuta võib olla äärmisel keeruline. Anonüümseuse puhul läheb sageli kaduma suur osa detaile ja täiesti anonüümne andmestik võib olla eesmärgi saavutamiseks sobimatu.

**TÄHTSUS**

**IKÜM põhjendus p 26**

IKÜM-is ei käsitleta anonüümse teabe töötlemist, sealhulgas statistilisel või uuringute eesmärgil.

Kindlasti tuleb meeles pidada, et pseudonümiseeritud andmed ei ole anonüümseid andmed ja anonüümse teabe koha käiv välistus kohaldub ainult kitsalt täiesti anonüümsele andmestikule.

## ISIKUANDMETE LIIGITAMINE TUNDLIKKUSE ALUSEL

### Tavalised isikuandmed

- teave inimese ehk füüsilise isiku (andmesubjekti) kohta, millega saab teda otse või kaudselt tuvastada
- NB! tunnused ja nende kombinatsioonid

### Tundlikud isikuandmed

- ei ole üldmääruses eraldi loetletud, kuid määratletavad kui isiku privaatelule suuremat ohtu valmistavate andmetena
- avaldamisega kaasneb oht elule ja tervisele, identiteedivargusele ning kui võib kaasneda varaline ja mainekahju

### Eriliiki isikuandmed

- on isikuandmed, 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 seksuaalelu ja seksuaalse sättumuse kohta

**Tavalised isikuandmed** on teave inimese ehk füüsilise isiku (andmesubjekti) kohta, millega saab teda otse või kaudselt tuvastada.

**Tundlikud isikuandmed** ei ole üldmääruses eraldi loetletud, kuid määratletavad kui isiku privaatelule suuremat ohtu valmistavate andmetena ning mis ei kuulu eriliiki isikuandmete loetellu. Kindlasti on tundlikeks isikuandmeteks ka mitteavalik teave inimese varandusliku seisuga kohta ja sotsiaalabi saamine. Seda tuleb kaaluda näiteks sotsiaalabi saamise tingimustele vastavuse süsteemide loomisel. Paljudel juhtudel osutub tundlikuks inimese kohta käiv info, mis on avaliku teabe seaduse alusel käsitletav kui juurdepääsupiiranguline teave.

Isikuandmete piiritlemine nn tavaliste ja tundlike isikuandmete puhul võib olla hägune. Näiteks üldiselt loetakse asukohaandmeid tavalisteks isikuandmeteks. Reaalajas asukoha tuvastust võimaldavad andmed on õiguskirjanduses liigitatud aga pigem tundlike isikuandmete alla.

**Eriliiki isikuandmete** alla kuuluvad enamasti selliseid andmeid, mis varasema sõnastuse järgi olid Eestis käsitletavad kui delikaatsed isikuandmed.

## Milliseid isikuandmeid nähtub fotolt?



## Kas tegemist on eriliiki isikuandmetega?

Seoses biomeetriliste andmetega tõusetub sageli küsimus, kas ka inimeste näo kujutised on biomeetrilised andmed. IKÜM põhjenduste kohaselt ei peeta näiteks fotode töötlemist isikuandmete eriliikide töötlemiseks. Näo kujutiste töötlemine on hõlmatud biomeetriliste andmete määratlusega üksnes juhul, kui neid töödeldakse konkreetsete tehniliste vahenditega, mis võimaldavad füüsilist isikut kordumatult tuvastada või autentida (vt IKÜM põhjendus p 51).



## Kas tegemist on isikuandmetega?

Tegemist on sünteetiliste andmetega ehk arvuti poolt genereeritud pildiga. Sellist inimest ei ole tegelikult olemas. Foto ei ole tehtud füüsilisest isikust ega seonu ühegi füüsilise isikuga. Tegemist ei ole isikuandmetega. Siiski ei ole seda võimalik tuvastada lihtsalt fotot vaadates. Inimsilma jaoks on sünteetilised andmed ja „päris“ isikuandmed sageli äravahetamiseni sarnased. Seega tasub sünteetiliste andmete kasutamisel kaaluda, kuidas hiljem tõendada, et tegemist on sünteetiliste andmetega ja töödeldud ei ole isikuandmeid.



## ANDMETE KOGUMITEST JÄRLDUSTE TEGEMINE



Seoses andmeanalüütikaga tuleb olla ettevaatlik isikuandmete kogumistes järelduste tegemisel. **Mida rohkem on andmeid, seda tõenäolisemaks muutub, et kogumisse satuvad või kogumist on järeldatavad ka eriliiki isikuandmed.** Näiteks võib andmestikust nähtuda religioosse asutuse perioodiline külastamine ja/või samale asutusele annetuste tegemine. Suure tõenäosusega on sel juhul selliste andmete töötlemisel ühtlasi töötlemisel eriliiki isikuandmed (isiku usulised veendumused).

**KAS JURIIDILISE ISIKU ANDMED  
ON ISIKUANDMED?**



## JURIIDILISE ISIKU ANDMED

- Ükski isik ei peaks nõudma üldmäärusega ette nähtud **kaitset** seoses selliste andmete töötlemisega, mis **puudutavad juriidilisi isikuid**, eelkõige:
  - juriidiliste isikutena asutatud ettevõtjaid,
  - juriidilise isiku nime ja vormi; ning
  - kontaktandmeid (nt e-post, telefon).
- **AKI seisukoht 2021:** Kuna isikuandmeteks on igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta, siis on **isikuandmeteks ka juriidilise isiku esindaja andmed** (nt nimi, isikukood, sünniaeg). **Andmekaitsereeglid ei kohaldu aga juriidilise isiku nimele ja kontaktandmetele.**

Isikuandmeteks on juriidilise isiku esindaja andmed (nt nimi, isikukood, sünniaeg), kuid andmekaitsereeglid ei kohaldu juriidilise isiku nimele ega kontaktandmetele.

## JURIIDILISE ISIKU ANDMED

Isikuandmete mõiste on lai, hõlmates mh olukorra, kus isik on tuvastatav kasutades seaduslikke vahendeid, mis võimaldavad kõnealuse isiku tuvastada tänu täiendavale teabele. [...] andmed äriühingute juhatuse liikmete kohta on veebis avalikult kättesaadavad, siis juhul, kui kohtulahend sisaldab andmeid, mille avaldamine võib oluliselt kahjustada juhatuse liikme eraelu puutumatus, tuleb **vajaduse korral asendada ka äriühingu nimi tähemärgiga ning jätta avaldamata registrikood või muud andmed, mis võimaldavad äriühingut identifitseerida**. Füüsilise isiku eraelu puutumatus tagamiseks ei tohi isik olla tuvastatav ka koostoimes muude veebiotsingutega.

Riigikohtu 04.04.2022 otsus kohtuasjas nr 3-21-2196 ja seal viidatud kohtupraktika.

Maksu- ja Tolliamet suurendas maksuotsusega ettevõtte X maksukohustust 26 332 euro võrra. X esitas halduskohtule kaebuse. Ettevõtte X asus seisukohale, et kohtumenetluses tehtud määruse avaldamine X-i juhatuse liikme tuvastamist võimaldavate andmetega kahjustas lubamatult tema [uhatuse liikme eraelu. Kahjulikud tagajärjed olid juba saanud, sest kohtulahendit kajastati ka meediaväljaandes.

HKMS § 175 lg-s 4 on sätestatud, et kui otsus sisaldab delikaatseid isikuandmeid või muid andmeid, mille avaldamine võib oluliselt kahjustada isiku eraelu puutumatus, ning eraelu puutumatus kahjustamist ei ole võimalik vältida ka sama paragrahvi lõikes 3 sätestatud järgides, avaldab kohus andmesubjekti taotlusel või omal algatusel otsuse ilma eraelu puutumatus kahjustavate andmeteta, avaldab üksnes otsuse resolutsiooni või ei avalda otsust. Nimetatud säte puudutab füüsilise isiku isikuandmete kaitset. Praegusel juhul esitas **HKMS § 175 lg 4 alusel taotluse juriidilisest isikust kaebaja oma seadusliku esindaja kui füüsilise isiku eraelu kaitseks**. Kohtu hinnangul oli sellises olukorras taotluse esitamine teise andmesubjekti õiguste kaitseks lubatav. Juriidiline isik kaitseb selliselt kaudselt ka enda huve. **Isikutel peab olema võimalik kohtusse pöörduda, kartmata, et nende või nendega seotud isikute, nt seadusliku esindaja kaitset vajav teave saab avalikuks**. Sellise kindlustunde puudumisel oleks kohtusse pöördumise õigust piirav toime. Kui isik jätab seepärast kohtusse pöördumata, et ta ei soovi, et avalikkus saaks teada kasvõi ainuüksi faktist, et tal on kohtuvaidlus, oleks andmete varjamata jätmisel kohtusse pöördumise õigust piirav toime.

**Kaebaja õiguste kaitseks asendati kaebaja nimi, st juriidilise isiku nimi, tähemärgiga.**

## MIS ON "TÖÖTLEMINE"?

- Isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum.

### Näiteks:

- kogumine,
- dokumenteerimine; korrastamine, struktureerimine,
- säilitamine, kohandamine ja muutmine,
- päringute tegemine, lugemine, kasutamine,
- edastamine, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine,
- ühitamine või ühendamine,
- piiramine, kustutamine või hävitamine.

Isikuandmete töötlemine on isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum.

KÜSIMUS: Andmete töötlemine teadusuuringute eesmärgil vs kas siis on piirang väliste avaandmete juurde liidestamisel?

Liidestamine on andmetöötlustoiming, st peab täitma kõik andmekaitse põhimõtted, sh õiguslik alus, minimaalsus, eesmärgipärasus, läbipaistvus jne.

## VASTUTAV VS VOLITATUD TÖÖTLEJA?

VASTUTAV  
töötleja

- Määrab üksi või koos teistega kindlaks isikuandmete töötlemise eesmärgid ja vahendid
- MIKS? KUIDAS?

VOLITATUD  
töötleja

- Töötleb isikuandmeid vastutava töötleja nimel

**Vastutav töötleja:** füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid; kui sellise töötlemise eesmärgid ja vahendid on kindlaks määratud liidu või liikmesriigi õigusega, võib vastutava töötleja või tema määramise konkreetsed kriteeriumid sätestada liidu või liikmesriigi õiguses.

Riik tervikuna ei ole vastutav töötleja. Samamoodi ei ole asutuse siseselt üldjuhul ametnik ise üksi vastutav töötleja. Võib olla mingi projekti juht, st selle projekti eest vastutav isik, aga see ei tähenda, et ta oleks vastutav töötleja IKÜM mõttes.

**Volitatud töötleja:** füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel.

Volitatud töötleja ei ole vastutava töötleja töötaja, vaid on teine isik, asutus või organ.

## ANDMEANALÜÜTIKA

### MINEVIK

- Kirjeldab asjaolude senist käiku

### OLEVIK

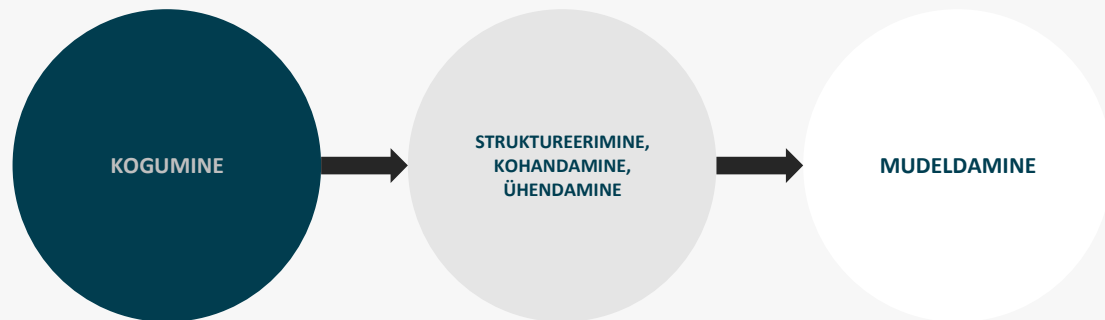
- Annab seniste asjaolude põhjal ülevaate, milline võiks olla edasine sündmuste käik

### TULEVIK

- Annab seniste asjaolude põhjal ülevaate, milline võiks olla edasine sündmuste käik ja kuidas ühe või teise tulemuse saavutamiseks toimida

Andmeanalüütika käsitlus käesoleva koolituse kontekstis. Andmeanalüütikal on mitmeid erinevaid kasutusvõimalusi. Andmeanalüütika abil võib uurida mineviku sündmusi, et jõuda selgusele, kuidas mingisse punkti jõuti. Samuti võib uurida, milline võiks seniste asjaolude põhjal olla sündmuste edasine käik. Kolmandaks ja võib-olla üheks kõige mõjusamaks andmeanalüütika võimaluseks on seniste asjaolude põhjal ennustada edasist sündmuste käiku ja prognoosida, kuidas ühe või teise tulemuse saavutamiseks peaks praeguses ajahetkes toimima.

## ANDMEANALÜÜTIKA – MUDELI EHITUS

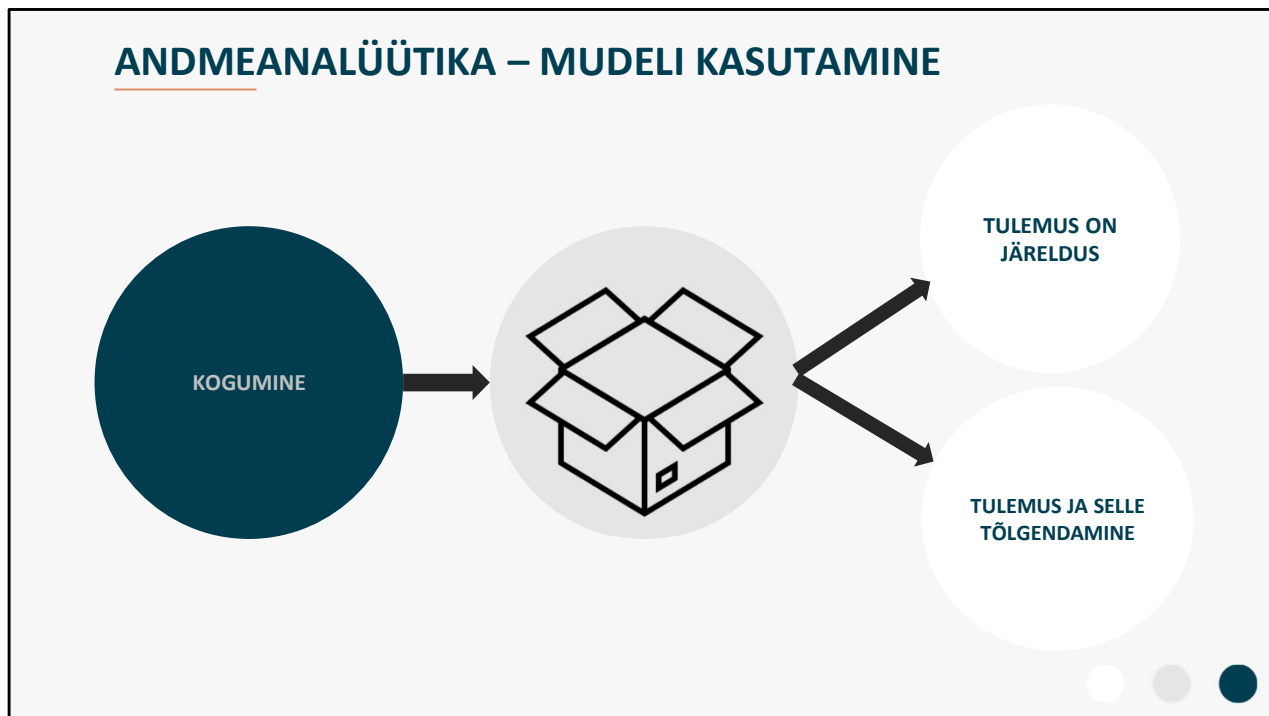


Isikuandmete töötlemise mõttes tasub andmeanalüütika toimingute käigus eristada erinevaid isikuandmete töötlemise toiminguid. Näiteks analüütilise mudeli loomisel on kindlasti vähemalt kolm selgelt eristatavat etappi (toimingut):

1. andmete kogumine;
2. andmete süstematiseerimine, kohandamine ja ühendamine analüütikaks sobiva andmekogumi loomiseks;
3. mudeldamine ehk automatiseeritud analüüs korrelatsioonide leidmiseks.

Oluline on tagada kõikide nende toimingute käigus isikuandmete kaitse põhimõtete järgimine. Selleks, et põhimõtteid järgida, on vaja mõista erinevate töötlemistoimingute sisu ja neid üksteisest selgelt eristada. Näiteks on andmete kogumise ja süstematiseerimise protsessis eriline tähtsus andmete õigsusel. Isikuandmed peavad olema õiged ja vajaduse korral ajakohastatud. Isikuandmete töötleja peaks võtma kasutusele mõistlikud meetmed tagamaks, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutaks või parandataks viivitamata. Kui andmeanalüütika esimestes etappides ei järgita isikuandmete kaitse põhimõtteid, siis järgmistes etappides probleemid kuhjuvad.



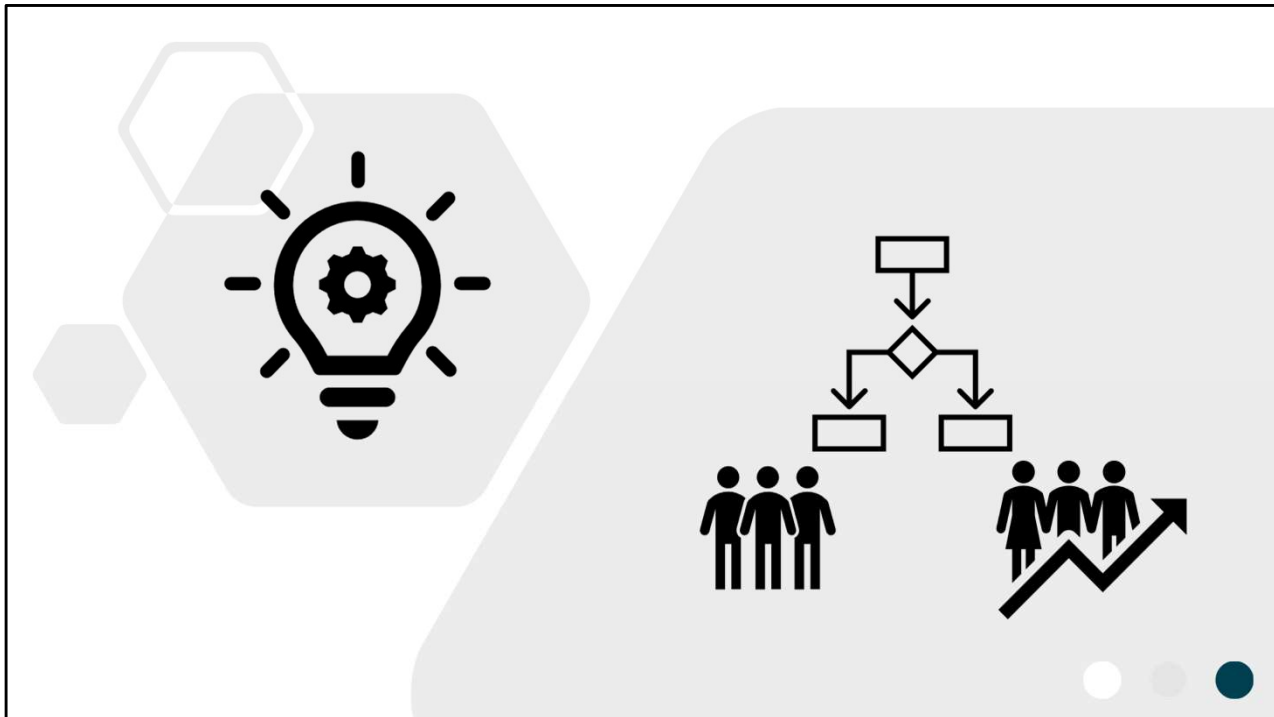


Eristades andmeanalüütika etappe, peaks mudelite kasutamisel isikuandmete töötlemise kontekstis eristama profiilianalüüsi ja andmete põhjal automatiseeritud otsuste tegemist.

**Profiilianalüüs** on menetlus, mis võib hõlmata hulka statistilisi järeldusi. **Üksnes automatiseeritud töötlusel põhinev otsuste** tegemine on otsustamine tehnoloogiliste vahendite abil ilma inimese sekkumiseta. Nende kohta on rohkem loengu II loengu jooksul.

Isikuandmete kaitse üldmäärusega on kehtestatud sätted tagamaks, et profiilianalüüs ja automatiseeritud töötlusel põhinevate üksikotsuste tegemine (olenemata sellest, kas see hõlmab profiilianalüüsi või mitte) ei mõjuta põhjendamatult üksikisikute õigusi; näiteks on kehtestatud:

- konkreetsed läbipaistvuse ja õigluse nõuded;
- suurem vastutus;
- töötlemise konkreetsed õiguslikud alused;
- üksikisikute õigus esitada vastuväide profiilianalüüsile ja eelkõige turunduse eesmärgil profiilianalüüsile ning
- teatavate tingimuste täitmise korral vajadus teha andmekaitsealane mõjuhinnang.

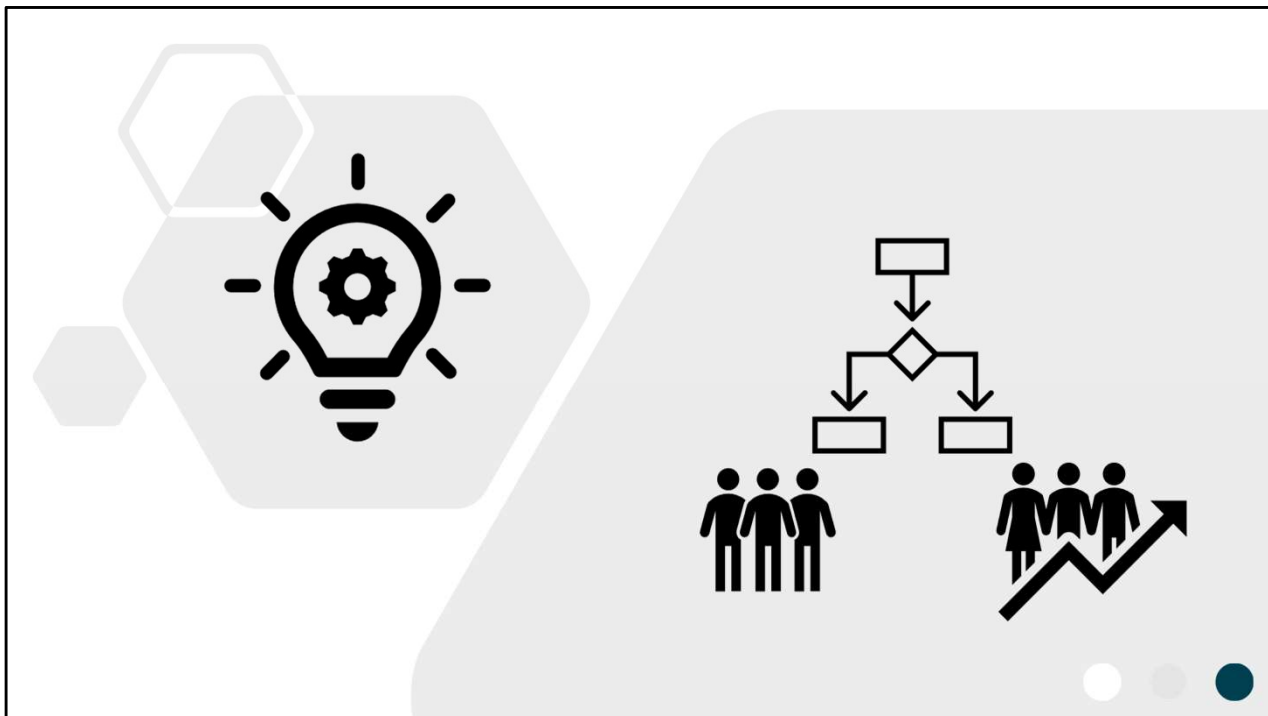


Nii mudeli ehitamisel kui ka selle kasutamisel peaks olema esmane küsimus, kas on üldse vaja isikuandmeid. Alati ei saa mitte isikustatud andmetega toimetada. Aga kui saab, siis tuleks seda eelistada. Samas ei tähenda see, et andmetega võib teha mida tahes.

Hooletu suhtumise näide on see, kui ei analüüsita nõuetekohaselt anonüümitud andmete teatavatel tingimustel avalduvat mõju üksikisikutele, eriti profileerimise korral. Üksikisiku eraelu puutumatus on kaitstud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 ning ELi põhiõiguste harta artikliga 7. Isegi kui andmekaitsealased õigusaktid ei ole anonüümitud andmete suhtes enam kohaldatavad, võivad anonüümitud ja kolmandatele isikutele kasutamiseks edastatud andmed vähendada eraelu puutumatust. Anonüümsete andmete käsitsemisel tuleb olla väga hoolikas, eeskätt juhul, kui neid kasutatakse (sageli kombineerituna muude andmetega) selliste otsuste tegemiseks, mis avaldavad (ka kaudselt) mõju üksikisikutele (vt ka: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_et.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_et.pdf)).

IKS § 6 lg 1: Isikuandmeid võib andmesubjekti nõusolekuta teadus- või ajaloouringu või riikliku statistika vajadusteks töödelda eelkõige pseudonüümitud või samaväärset andmekaitse taset võimaldaval kujul. Enne isikuandmete üleandmist teadus- või ajaloouringu või riikliku statistika vajadustel töötlemiseks asendatakse isikuandmed pseudonüümitud või samaväärset andmekaitse taset võimaldaval kujul andmetega.

*Jätkub (1/2)*



*Jätk (2/2)*

IKS § 6 lg 3: Teadus- või ajaloouringu või riikliku statistika vajadusteks andmesubjekti nõusolekuta tema kohta käivate andmete töötlemine andmesubjekti tuvastamist võimaldaval kujul on lubatud üksnes juhul, kui on täidetud järgmised tingimused:

- 1) pärast tuvastamist võimaldavate andmete eemaldamist ei ole andmetöötlemise eesmärgid enam saavutatavad või neid oleks ebamõistlikult raske saavutada;
- 2) teadus- või ajaloouringu või riikliku statistika tegija hinnangul on selleks ülekaalukas avalik huvi;
- 3) töödeldavate isikuandmete põhjal ei muudeta andmesubjekti kohustuste mahtu ega kahjustata muul viisil ülemäära andmesubjekti õigusi.

Kui teadus- või ajaloouring põhineb eriliiki isikuandmetel, siis kontrollib asjaomase valdkonna eetikakomitee või AKI. Kohaldub ainult isikustatud kujul eriliiki isikuandmete puhul. Eetikakomitee või AKI luba ei ole vaja, kui esmalt andmed pseudonüümitakse või anonüümitakse.

NB! Statistiline eesmärk eeldab, et töötlemise tulemus ei ole isikuandmed, vaid koondandmed, ning et seda tulemust või isikuandmeid ei kasutata ühtegi konkreetset füüsilist isikut puudutavate meetmete või otsuste toetamiseks.



## ISIKUANDMETE TÖÖTLEMISE ÜLDPÕHIMÕTTED

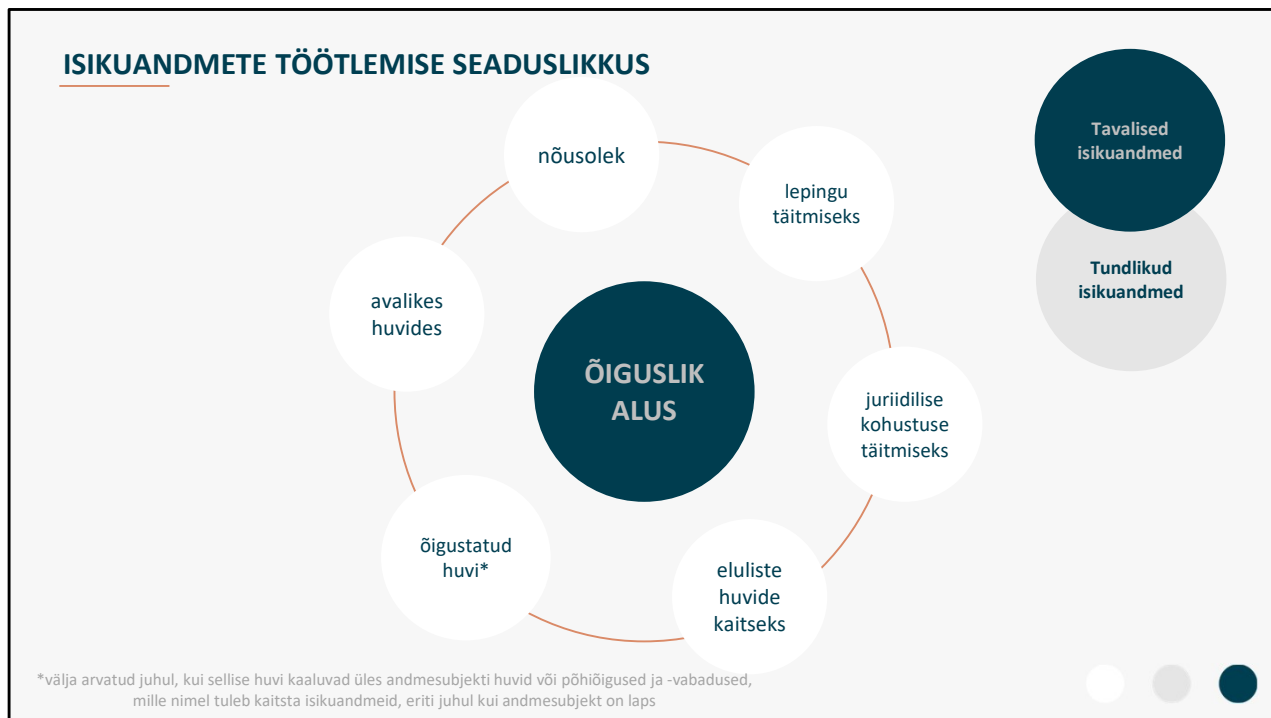
- seaduslikkus, õiglus ja läbipaistvus
- eesmärgi piirang
- võimalikult väheste andmete kogumine
- õigsus
- säilitamise piirang
- usaldusväärsus ja konfidentsiaalsus



Kui uuringuks, analüüsiks või mistahes muuks toiminguks on vaja kasutada isikuandmeid, siis kohalduvad kõik IKÜM põhimõtted ja neist tulenevad kohustused. Artikkel 5 loetleb põhimõtted.

NB! Käesoleva koolituse kontekstis antud tõlgendus põhimõtetele on üks võimalik paljudest võimalikest tõlgendustest. Käesoleva koolituse raames antud soovitusi ei saa käsitleda õigusnõuna. Olenevalt konkreetse juhtumi asjaoludest, võib tõlgendus üldpõhimõtetele erineda käesoleval koolitusel arutatust.

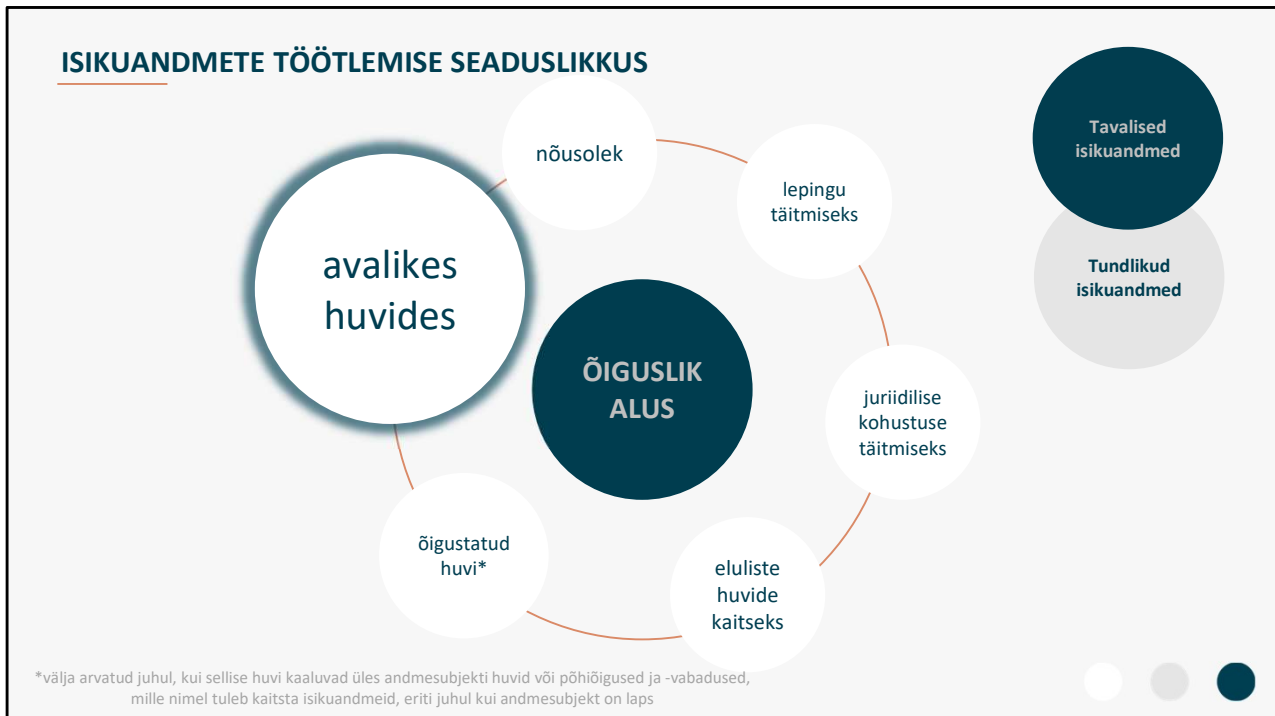
Andmeanalüütika puhul tõusetub väga sageli küsimus töötlemistoimingu õigusliku aluse korrektse valiku ehk seaduslikkusega seoses. Samuti tuleb leida tasakaal vajalike, kuid samas võimalikult väheste, andmete kogumise vahel. Keskendume koolituse käigus eelkõige nendele põhimõtetele.



Isikuandmete töötlemise seaduslikkus tähendab, et töötlemiseks peab olema õiguslik alus. Õigusliku aluse olemasolu aetakse praktikas sageli segamini eesmärgiga. See, et on olemas eesmärk, ei tähenda, et on olemas õiguslik alus. Eesmärk ei pühitse abinõud. Isikuandmete töötlemise õiguslikud alused on loetletud IKÜM artikli 6 lõikes 1 (lisaks isikuandmete eriliikide kohta IKÜM artikli 9 lõikes 2).

Erinevad andmetöötlemise õiguslikud alused võivad eksisteerida kõik kõrvuti ühe ja sama andmesubjektiga tekkinud suhte raames. Neid tuleb eristada andmekoosseisude kaupa, tuues selgelt välja missuguseid andmeid millisel õiguslikul alusel töödeldakse.

Kohalik õigus ei lisa aluseid, vaid täpsustab neid. Näiteks on õigusaktis sätestatud avalikes huvides olev ülesanne. Või on täpsustatud õigustatud huvi (IKS – ajakirjandus, kunstiline eneseväljendus, riikliku statistika ja arhiveerimine jne).



Isikuandmete töötlemine on seaduslik, kui see on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks. Töötlemise alus peaks olema sätestatud liidu või liikmesriigi õigusaktis. Iga üksiku isikuandmete töötlemise toimingu reguleerimiseks ei pea olema eraldi õigusakti – erinevad toimingud võivad olla kantud üldisest eesmärgist.

Avaliku võimu teostamiseks peetakse õigusaktides sätestatud avaliku võimu funktsioonide teostamist.

Avalikes huvides oleva ülesande täitmiseks peetakse õigusaktides sätestatud ülesannete täitmist.

Töötlemine peab olema vajalik selleks konkreetseks eesmärgiks. Kui eesmärki on võimalik saavutada muude vahenditega, siis ei ole toiming vajalik. Eelkõige ei ole toiming vajalik, kui sama tulemust oleks võimalik saavutada ilma isikuandmeid töötlemata või oluliselt väiksemas ulatuses isikuandmete töötlemisega.

## AVALIKU VÕIMU TEOSTAMINE

- Avaliku võimu teostamine ATS § 7 lg 3 (osaline loetelu):
  - ametiasutuse juhtimine
  - riikliku ja haldusjärelevalve teostamine
  - riigi julgeoleku ja põhiseadusliku korra tagamine
  - Riigikogu, Vabariigi Presidendi, Riigikontrolli, õiguskantsleri ja kohtute põhiülesannete täitmiseks vajalike otsuste tegemine, nende sisuline ettevalmistamine või rakendamine
  - Vabariigi Valitsuse, kohaliku omavalitsuse üksuse volikogu, valla- või linnavalitsuse ja ametiasutuse pädevuses olevate poliitikat kujundavate otsuste sisuline ettevalmistamine või rakendamine

Näide avaliku võimu teostamisest. Sätestatud avaliku teenistuse seaduses.

## AVALIKES HUVIDES OLEV ÜLESANNE

- avaliku ülesande definitsiooni seaduses ei ole
- tõlgendamise kriteeriumid on kujunenud kohtupraktikas ja õiguskirjanduses
- õigusliku aluse valik vajab igakordset tõlgendamist ja põhjendamist

Avalikes huvides oleva ülesande ühest definitsiooni Eesti õigusaktides ei ole. Tegemist on avatud õigsmõistega, mida tuleb sisustada tõlgendades. Näiteks on kohtupraktikas välja toodud järgnevad seisukohad:

Senises praktikas on korduvalt rõhutatud, et avalik ülesanne peab olema ette nähtud vahetult seadusega või seaduse alusel või olema tõlgendamise teel õigusnormist tuletatav (Riigikohtu erikogu määrus asjas nr 3-3-4-1-10, p 5; halduskolleegiumi otsus asjas nr 3-3-1-72-11, p 8; kriminaalkolleegiumi otsus asjas nr 3-1-1-98-15, p-d 61 ja 62; otsus nr 1-16-9105/108, p 44).

Avalik huvi mingi teenuse olemasolu vastu iseenesest ei muuda veel seda teenust avalikuks ülesandeks. Kui eraisik osutab teenust vabatahtlikult (nt eralasteaed), nt turul valitseva nõudluse rahuldamiseks, ei täida ta avalikku ülesannet. Avalikuks ülesandeks muutub teenus seega siis, kui seda osutatakse avalik-õigusliku isiku seadusest tuleneva kohustuse täitmiseks (Riigikohtu halduskolleegiumi otsus kohtuasjas nr 3-3-1-19-14, p 12).

Avalike ülesannete puhul reguleerib avalik õigus tihti soorituse tegemise kohustust, kuid sooritus ise võib alluda eraõiguslikule regulatsioonile. Nii on see näiteks vanglapoe pidamisel – kohustus tagada kinnipeetavale sisseostude tegemise võimalus on avalik ülesanne, samas kui vanglapoes kaupade ostmine toimub eraõigusliku müügilepingu alusel (ning seejuures ei ole vahet, kas kauplust peab vangla ise või on ta selle ülesande delegeerinud eraõiguslikule isikule (Riigikohtu halduskolleegiumi otsus kohtuasjas nr 3-3-1-72-11, p 10-11).



## AVALIKES HUVIDES OLEV ÜLESANNE

### Eesti Haigekassa seadus

#### § 2. Haigekassa eesmärk ja ülesanded

(1) Haigekassa eesmärk on ravikindlustushüvitiste võimaldamine, tervishoiuteenuste eest tasumine ning tervishoiuteenuste korraldamisega seotud teiste ülesannete täitmine vastavalt ravikindlustuse seadusele, tervishoiuteenuste korraldamise seadusele ja muudele õigusaktidele ning haigekassa eelarves ettenähtud kuludele.

[RT I, 28.12.2017, 4 - jõust. 01.01.2018]

(2) Oma eesmärgi saavutamiseks täidab haigekassa järgmisi ülesandeid:

1) korraldab ravikindlustust, tervishoiuteenuste eest tasumist ning tervishoiuteenuste korraldamisega seotud teiste ülesannete täitmist, tagades haigekassa eelarve efektiivse ja otstarbeka kasutamise;

2) täidab ravikindlustuse seadusest, tervishoiuteenuste korraldamise seadusest ja muudest õigusaktidest tulenevaid ülesandeid;

3) peab ravikindlustushüvitiste võimaldamiseks ja käesolevast seadusest, ravikindlustuse seadusest, tervishoiuteenuste korraldamise seadusest ning muudest õigusaktidest tulenevate muude ülesannete täitmiseks haigekassa andmekogu;

[RT I, 13.03.2019, 2 - jõust. 15.03.2019]

3<sup>1</sup>) teavitab isikuid haigekassa põhikirjas sätestatud korras elektrooniliselt või muul viisil ravikindlustuse seadusest või muudest õigusaktidest tulenevatest õigustest ja kohustustest;

[RT I, 13.03.2019, 2 - jõust. 15.03.2019]

4) kontrollib haigekassa poolt osaliselt või täielikult tasutavate teenuste kvaliteeti ja põhjendatust;

5) korraldab ravikindlustust ja tervishoiuteenuse osutamist ning haigekassat puudutavate välislepingute täitmist;

6) osaleb tervishoiu planeerimisel ning avaldab arvamust haigekassaga, ravikindlustusega ja tervishoiuteenuste korraldusega seonduvate õigusaktide ja välislepingute eelnõude kohta;

7) annab nõu ravikindlustusega seonduvates küsimustes;

8) annab nõu tervishoiuteenuste korraldamise seadusest ja muude õigusaktidest seonduvates küsimustes;

Näiteks – Haigekassa kasutab nn kratti krooniliste haigete tervise ja ravivajaduste ennustamismudelit. Kuigi ei krati kasutamine ega vastava ennustamismudeli ehitamine ei ole sõna-sõnalt kirjas Haigekassa ülesandena Eesti Haigekassa seaduses, siis on see olemuslikult siiski seotud seaduses sätestatud ülesannetega. Riskipõhise ravijuhtimisega on võimalik perearstidel tuvastada oma nimistus mitme kroonilise haigusega patsiendid, kelle puhul täiendav ennetus, nõustamine ja jälgimine tooks enim kasu nende tervisele ja elukvaliteedi paranemisele.

Loe veel: <https://www.kratid.ee/haigekassa-kasutuslugu>

## ASUTUSTE KOOSTÖÖ - AMETIABI

### Halduskoostöö seadus

#### § 17. Ametiabi

(1) Haldusorgan annab käesolevas seaduses sätestatud alustel ja korras akti või sooritab toimingu oma pädevuse piires teise haldusorgani taotlusel selle haldusorgani ülesande täitmise toetamiseks (ametiabi).

(2) Ametiabi sätteid ei kohaldata:

- 1) alluvussuhtele,
- 2) kui abi andmise kohustus on haldusorganile ette nähtud seadusega.

#### § 18. Ametiabi taotlemise ja andmise alused

(1) Haldusorgan võib taotleda teiselt haldusorganilt ametiabi, kui:

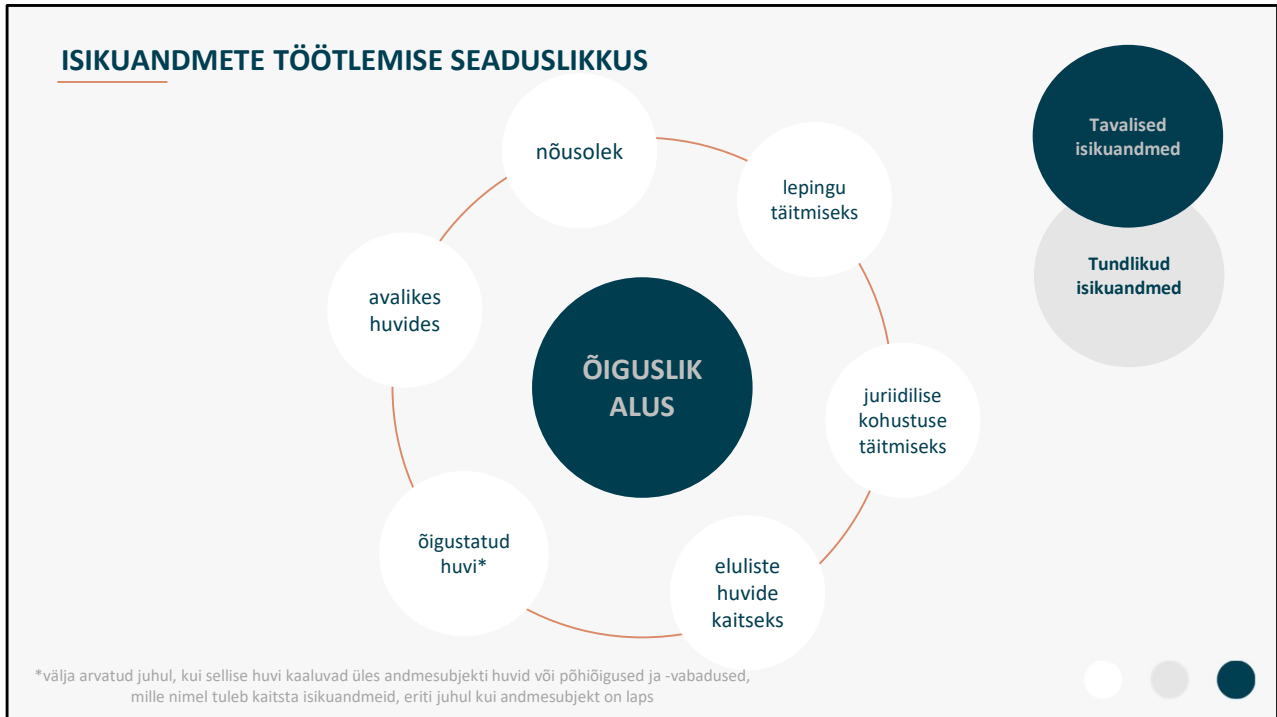
- 1) haldusülesande täitmiseks vajaliku akti andmine või toimingu sooritamine ei ole tema pädevuses;
- 2) haldusülesande täitmiseks on vaja andmeid, mis haldusorganil puuduvad või mida haldusorgan ei ole võimeline välja selgitama;
- 3) haldusülesande täitmiseks on vaja teise haldusorgani valduses olevaid dokumente või muid tööandeid;
- 4) haldusorgan ei saa akti anda või toimingut sooritada muul põhjusel;
- 5) ametiabi kasutamine oleks majanduslikult oluliselt soodsam kui mittekasutamine.

Senini on õiguskirjanduses oldud ametiabi ja selle raames isikuandmete jagamise osas pigem konservatiivsel seisukohal (refereeritud I. Pilvingu artiklist "Ametiabi", Juridica nr 2015/3, lk 177-183):

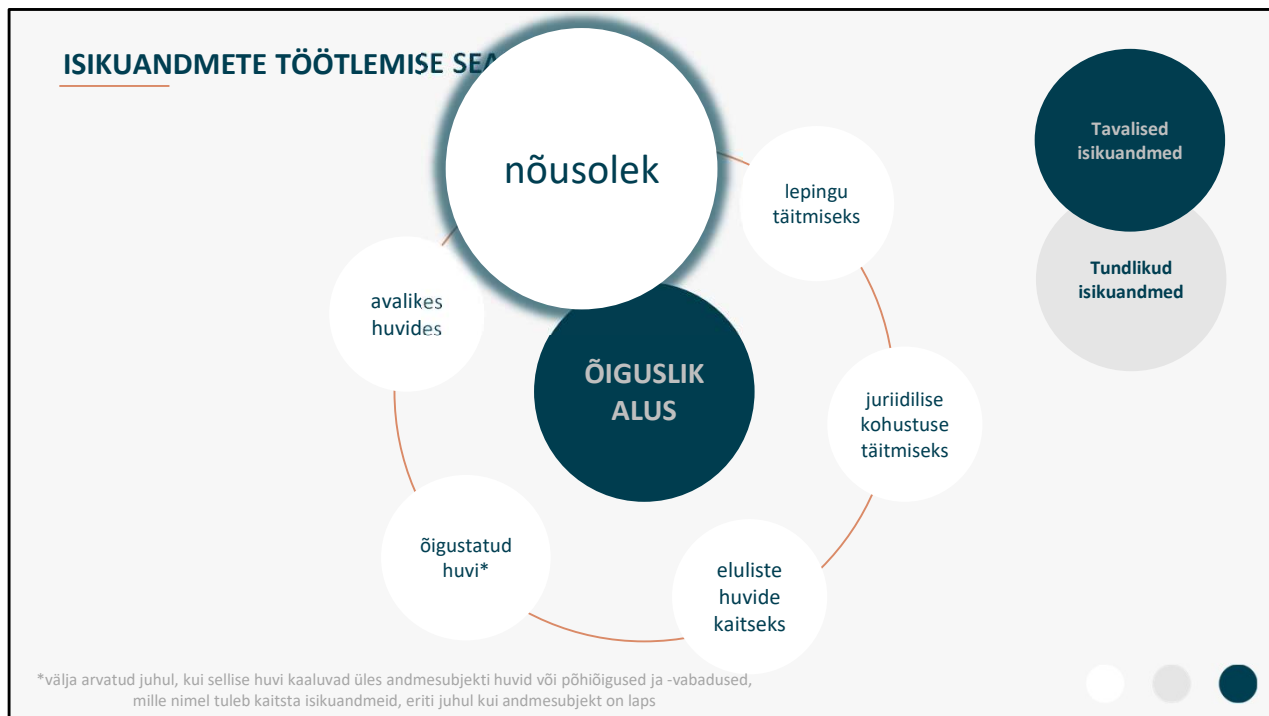
Ametiabi üks kandvaid eesmärke oli vähendada halduskorralduse killustatust ja parandada asutuste vahelist koostööd. Siiski tuleb ametiabi andmisel piirduda üksikjuhtumiga. Ametiabiks ei peeta süstemaatilist ja kestvat abistamist, näiteks regulaarset teabevahetust, pidevat juurdepääsu teise asutuse andmekogudele ja kestvat kohustust vastata teiste asutuste päringutele. Püsiv koostöö ei saa toimuda HKTS 3. peatüki alusel, see võib vajada eraldi regulatsiooni. Süstemaatiline koostöö ja ametiabi võivad ka omavahel põimuda. Samas on märgitud, et ametiabi ülesanne on tasandada haldusorganisatsiooni funktsiooni- ja pädevusjaotusest tulenevat killustatust avaliku halduse toimimisel. Ametiabi aitab seega tagada riigivõimu ühtsust, võimaldab kasutada teise asutuse volitusi ja ressursse nende dubleerimise asemel, aitab vältida topelttööd, teenides nõnda lihtsa, eesmärgipärase, ökonoomse ja kiire menetluse eesmärki.

Seoses koroonapandeemiaga tõusetus aga 2020. aastal vajadus näiteks andmevahetuseks Terviseameti ja PPA vahel. Andmekaitse Inspeksioon asus seisukohale, et muuhulgas on selline andmevahetus õiguspärane ametiabi raames.

Loe täpsemalt AKI 2020 aastaraamat, lk 26. Kättesaadav: [https://aastaraamat.aki.ee/sites/default/files/aastaraamatud/aastaraamat\\_2020.pdf](https://aastaraamat.aki.ee/sites/default/files/aastaraamatud/aastaraamat_2020.pdf).





Avalik huvi on avalikus sektoris isikuandmete töötlemisel kindlasti peamine alus, kuid ei ole samas ainus alus. Suure tõenäosusega on lisaks üksikutel juhtudel asjakohased nii andmesubjekti nõusolek kui ka õigustatud huvi.



Andmesubjekti nõusolek tähendab, et andmesubjekt on andnud nõusoleku töödelda oma isikuandmeid ühel või mitmel konkreetsel eesmärgil. See ei pruugi olla avalikus sektoris isikuandmete töötlemiseks sageli kõige sobivam alus, sest õigussuhte osapooled ei ole võrdsel positsioonil (sama probleem nt töösuhtes).

Andmekaitse Inspektsioon on senini olnud seisukohal, et avalikus sektoris võib nõusoleku alusel isikuandmeid töödelda selliste juhtumite puhul, kus isikul on tõesti õigus otsustada oma andmete töötlemise üle kartmata kahjulikke tagajärgi. Selliseks olukorraks võib pidada eeskätt mugavusteenuseid.

## NÕUSOLEK

MAKSU- JA TOLLIAMET

ISIKUANDMETE AVALIKKUSELE KATTESAADAVAKS TEGEMINE

### RAHULOLUKÜSITLUS

Kaks korda aastas küsime klientidelt arvamust, kellel oli hiljutine kogemus meie e-teenuste keskkonna e-MTA teenuste kasutamisega või kes külastasid meie teenindusbürood, hellistasid või kirjutasid meie klienditoele.

Kasutajatelt saadud tagasiside on meile väga oluline ja aitab meil paremini näha oma teenuseid ja teeninduskvaliteeti läbi teie silmade. Nii oskame paremini hinnata, mis on juba hästi ja mida tuleks veel arendada, et pakkuda ootustele vastavat parimat kogemust.

Rahulolu mõõtmise veebikeskkonna teenust pakub meile lepingupartner OÜ Recommender. Kasutame rahulolu mõõtmiseks soovitusindeksi meetodikat.

Küsimustikule vastamine on vabatahtlik, küsitluste saamisest on võimalik loobuda, vajutades e-kirja teel saadetud küsimustiku lõpus olevale lingile „Eemalda meiliaadress nimekirjast“.

Klientide vastused säilitame Recommy veebikeskkonnas ilma isikuandmeteta kaks aastat. See on vajalik selleks, et võrrelda jooksva aasta tulemusi eelmise aasta tulemustega.

MEILE TEENISTUSSE KANDIDEERIMINE

Nõusoleku alusel saab edastada uudiskirju, korraldada rahuloluküsimustikke jne.

Saab teha ka uuringuid. Sellele viitab otseselt IKS § 6 sõnastus: Isikuandmeid võib andmesubjekti nõusolekuta teadus- või ajaloouringu või riikliku statistika vajadusteks töödelda [...]. Tuleb aga meeles pidada, et sul juhul kohalduvad nõusolekule ranged reeglid, mida ei pruugi olla lihtne täita.

## NÕUSOLEKU ANDMISE TINGIMUSED

- Kui töötlemine põhineb nõusolekul, peab vastutaval töötlejal olema võimalik **tõendada**, et andmesubjekt on nõustunud oma isikuandmete töötlemisega
  - selge kinnitusena
  - vabatahtlik
  - konkreetne ja ühemõtteline
  - muudest küsimustest selgelt eristatav
  - arusaadaval ja lihtsasti kättesaadaval kujul, kasutades selget ja lihtsat keelt

Nõusolek tuleks anda selge kinnitusena, näiteks kirjaliku kinnituse vormis, sealhulgas elektroonilisel teel, või suulise avaldusena, millega andmesubjekt annab vabatahtlikult, konkreetselt, teadlikult ja ühemõtteliselt nõusoleku teda puudutavate isikuandmete töötlemiseks. See võiks hõlmata vajaliku lahtri märgistamist veebisaidil, infoühiskonna teenuste tehniliste seadmete valimist või muud avaldust või käitumist, millest selles kontekstis konkreetselt nähtub andmesubjekti nõusolek teda puudutavate isikuandmete kavandatavaks töötlemiseks. Vaikimist, eelnevalt märgistatud lahtreid või tegevusetust ei tohiks seega pidada nõusolekuks. Nõusolek peaks hõlmama kõiki samal eesmärgil või samadel eesmärkidel tehtavaid isikuandmete töötlemise toiminguid. Kui töötlemisel on mitu eesmärki, tuleks nõusolek anda kõigi nende kohta (IKÜM põhjendus p 32).

Nõusolekut ei tohiks lugeda vabatahtlikult antuks, kui andmesubjektil pole tõelist või vaba valikuvõimalust või ta ei saa kahjulike tagajärgedeta nõusoleku andmisest keelduda või seda tagasi võtta (IKÜM põhjendus p 42). Selle tagamiseks, et nõusolek on antud vabatahtlikult, ei tohiks nõusolek anda isikuandmete töötlemiseks kehtivat õiguslikku alust konkreetsel juhul, kui andmesubjekt ja vastutav töötleja on selgelt ebavõrdses olukorras, eriti juhul kui vastutav töötleja on avaliku sektori asutus, ning seega on ebatõenäoline, et nõusolek anti selle konkreetse olukorra kõigi asjaolude puhul vabatahtlikult. Nõusolekut ei loeta vabatahtlikuks, kui ei ole võimalik anda erinevatele isikuandmete töötlemise toimingutele eraldi nõusolekut, ehkki see on üksikutel juhtudel asjakohane, või kui lepingu täitmine, sealhulgas teenuse osutamine, on pandud sõltuma sellisest nõusolekust, ehkki see ei ole lepingu täitmiseks vajalik (IKÜM põhjendus p 43).

## NÕUSOLEKU ANDMISE TINGIMUSED

- Kui töötlemine põhineb nõusolekul, peab vastutaval töötlejal olema võimalik **tõendada**, et andmesubjekt on nõustunud oma isikuandmete töötlemisega
- selge kinnitusena
- vabatahtlik
- konkreetne ja ühemõtteline
- muudest küsimustest selgelt eristatav
- arusaadaval ja lihtsasti kättesaadaval kujul, kasutades selget ja lihtsat keelt

*Jätk (2/3)*

Andmeanalüütika puhul võib olla keeruline nõusoleku küsimiseks piisavalt läbipaistvat teavet esitada. Samuti võib olla raskendatud õigel ajal andmesubjekti informeerimine. Nt kui varem kogutud andmeid soovitakse töödelda uuel eesmärgil.

Teadusuuringute kontekstis on lubatud teataval määral paindlikkust seoses nõusoleku spetsiifilisuse ja detailsuse määraga. Isikuandmeid kogudes ei pruugi teadlased suuta täielikult kindlaks teha nende töötlemise kõiki eesmärke. Sellisel juhul saavad nad paluda üksikisikutel anda nõusolek teatavate uurimisvaldkondade või teadusprojektide osade kohta. Nõusoleku põhielemendid peavad siiski olema täidetud: vabatahtlikult antud, teadlik, küsitud selge kinnitusena ja konkreetne kõnealuse teadusuuringu puhul võimalikul määral. Samuti peavad teadlased kindlasti järgima oma uurimisvaldkonna tunnustatud eetikanorme ja metoodikat.

Sellel teemal saab veel infot IKÜM põhjenduste punktist 33. Samuti tasub lugeda Euroopa Komisjoni seisukohta: [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/how-consent-processing-scientific-research-obtained\\_et](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/how-consent-processing-scientific-research-obtained_et).

*Jätkub (2/3)*

## NÕUSOLEKU ANDMISE TINGIMUSED

- Kui töötlemine põhineb nõusolekul, peab vastutaval töötlejal olema võimalik **tõendada**, et andmesubjekt on nõustunud oma isikuandmete töötlemisega
- selge kinnitusena
- vabatahtlik
- konkreetne ja ühemõtteline
- muudest küsimustest selgelt eristatav
- arusaadaval ja lihtsasti kättesaadaval kujul, kasutades selget ja lihtsat keelt

*Jätk (3/3)*

Seega võib teadusprojektis võib kasutada isikuandmeid nõusolekule tuginedes vaid juhul, kui projektil on hästi kirjeldatud eesmärk. Juhuks kui teadusprojekti raames toimuva andmetöötamise eesmärgi ei ole võimalik kohe alguses kindlaks määrata, nähakse põhjendusega 33 ette erand, mille kohaselt eesmärki võib kirjeldada üldisemalt. Teadusuuringute edenedes on võimalik hankida nõusolek projekti järgmiste etappide jaoks, enne kui need algavad.

Kui teadusuuringu asjaolud ei võimalda saada konkreetset nõusolekut, on täiendav kaitsemeede läbipaistvus. Eesmärgi täpse kirjelduse puudumist võib korvata korrapärase teabe, mille vastutav töötleja edastab teadusprojekti edenedes eesmärgi arenemise kohta, nii et aja jooksul muutub nõusolek võimalikult konkreetseks. Sellise teabe edastamise korral on andmesubjektil olukorrast vähemalt elementaarne ülevaade, mis võimaldab tal hinnata, kas näiteks kasutada õigust võtta nõusolek tagasi.

Loe veel:

[https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_et.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_et.pdf)



## NÕUSOLEKU ANDMISE TINGIMUSED

- Andmesubjektil on õigus nõusolek **igal ajal tagasi võtta**
- See ei mõjuta enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust
  
- NB! Tagasivõtmise õigusest peab teavitama

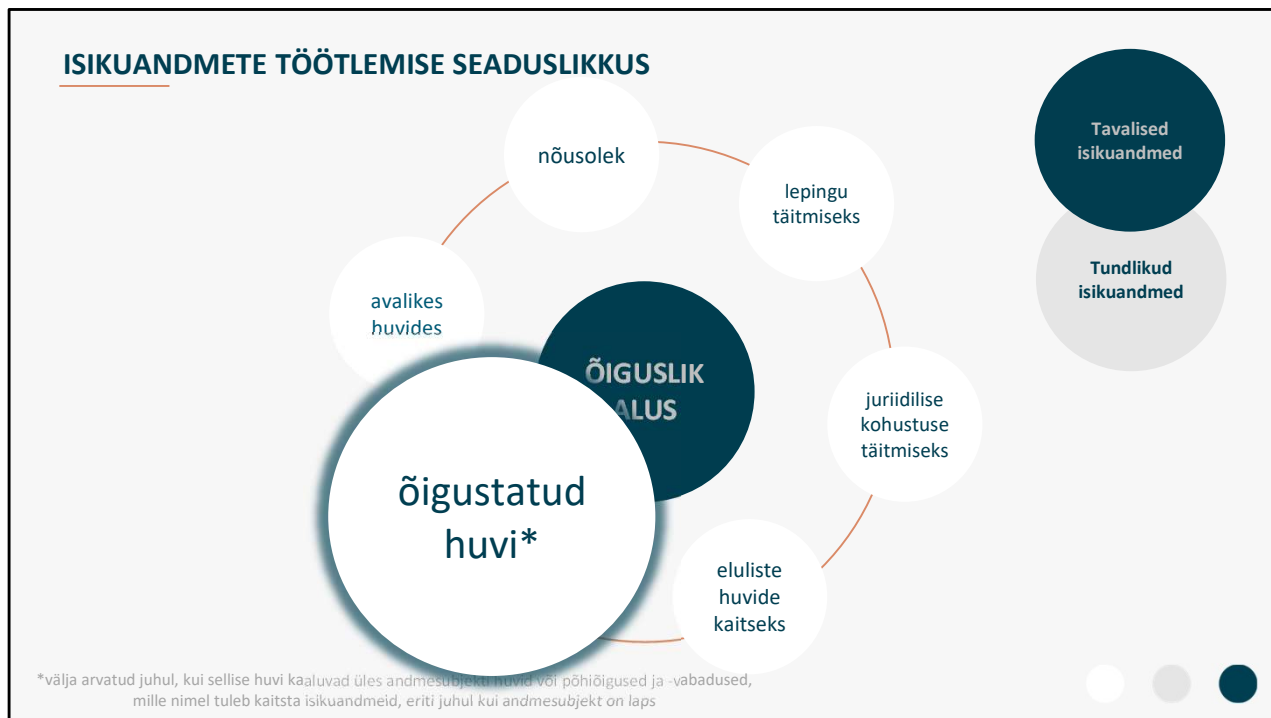
Andmesubjektil peab olema õigus oma nõusolek igal ajal tagasi võtta. Nõusoleku tagasivõtmise järel tuleb isikuandmete töötlemine viivitamatult lõpetada. Andmesubjekti peab nõusoleku tagasivõtmise õigusest teavitama enne nõusoleku andmist. Samuti peab andmesubjektile olema eelnevalt selgitatud, et nõusoleku tagasivõtmine ei mõjuta enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust. Nõusoleku tagasivõtmine peab andmesubjekti jaoks olema sama lihtne kui selle andmine (vt ka nõusoleku andmise tingimused, IKÜM artikkel 7). Kui selle isiku andmed on mingi mudeldamise andmestiku osa, siis võib olla keeruline neid sealt „välja võtta“, kuid mingit erandit uuringute puhuks IKÜM ette ei näe.

Kuigi IKS ja IKÜM lubavad teadusuuringute puhul piirata teatavaid andmesubjekti õigusi (IKÜM artiklites 15, 16, 18 ja 21 sätestatud andmesubjekti õigusi piirata niivõrd, kuivõrd nende õiguste teostamine tõenäoliselt muudab võimatuks teadus- või ajaloouringu või riikliku statistika eesmärgi saavutamise või takistab seda oluliselt), siis nõusoleku osas erandit ei ole.

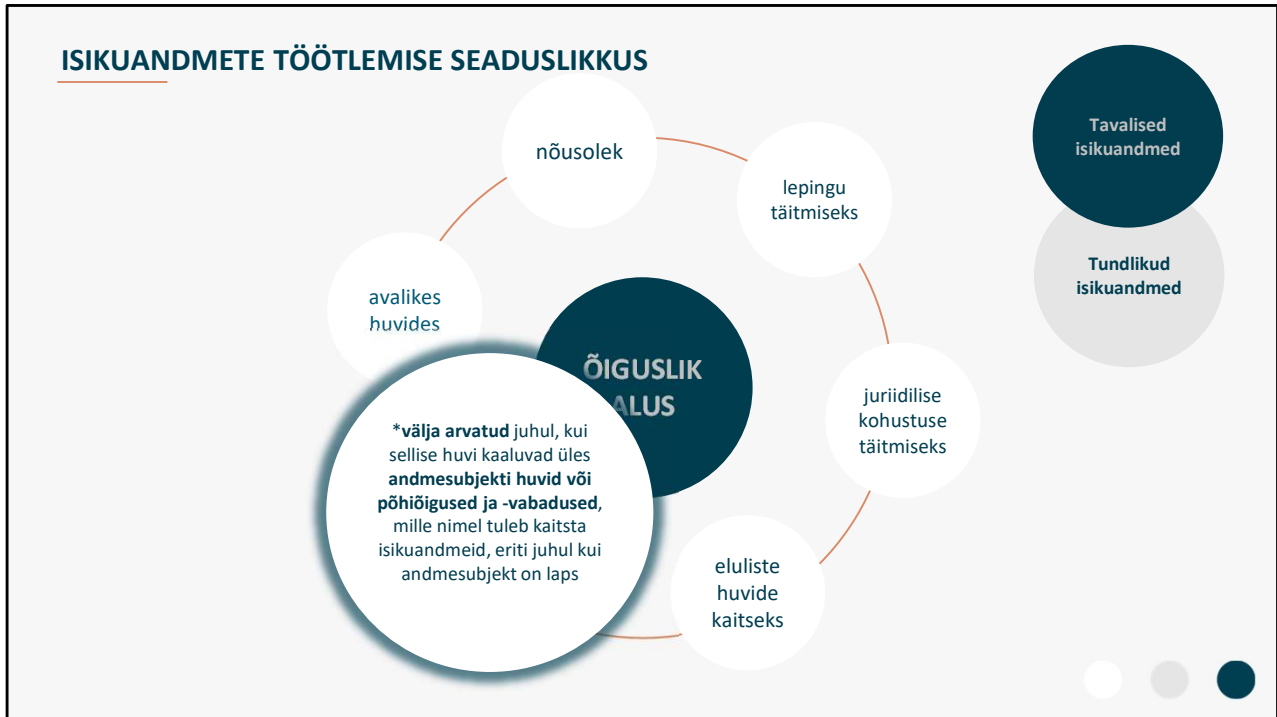
Andmekaitsekoogu märgib, et nõusoleku tagasivõtmine võib seada ohtu sellist liiki teadusuuringud, mille jaoks on vaja andmeid, mida on võimalik siduda üksikisikutega. Paraku on isikuandmete kaitse üldmääruses selgelt sätestatud, et nõusoleku saab tagasi võtta, ja vastutavad töötledjad peavad tegutsema sellest lähtuvalt – teadusuuringute puhul ei tehta sellest nõudest mingit erandit.

Loe veel:

[https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_et.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_et.pdf).



Õigustatud huvi ei ole võimalik õigusliku alusena kohaldada, kui isikuandmeid töötleb avaliku sektori asutus oma ülesannete täitmisel (vt IKÜM artikkel 6 lg 1). Siiski võib ka avaliku sektori toimingutes esineda erandeid ülesannete "kõrval". Juhul, kui tegemist ei ole otseselt avaliku ülesande täitmisega, ei ole välistatud ka selle õigusliku aluse kasutamine. Siiski on tegemist pigem erandlike olukordadega. Andmeanalüütika kontekstist võib selline alus osutada kohaldatavaks, kui töötlemisel on eesmärk väljaspool vajadust täita avalikku ülesannet.



Õigustatud huvi alusel ei tohi isikuandmeid töödelda, kui õigustatud huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb kaitsta isikuandmeid, eriti juhul kui andmesubjekt on laps. Selleks, et vastutava töötaja õigustatud huvi andmesubjekti huvid ja põhiõigustega võrrelda, tuleb läbi viia huvide kaalumine.

## ÕIGUSTATUD HUVI KOLMEASTMELINE KONTROLL

- 1. Mis on õigustatud huvi?** Mis huvi? Kelle huvi? Kas isikuandmete töötlemine on vajalik?
- 2. Mis on andmesubjekti õigused ja huvid?**
- 3. Huvide kaalumine.** Kumb huvi on olulisem? Miks?

NB! Kaalumise tulemus dokumenteerida.

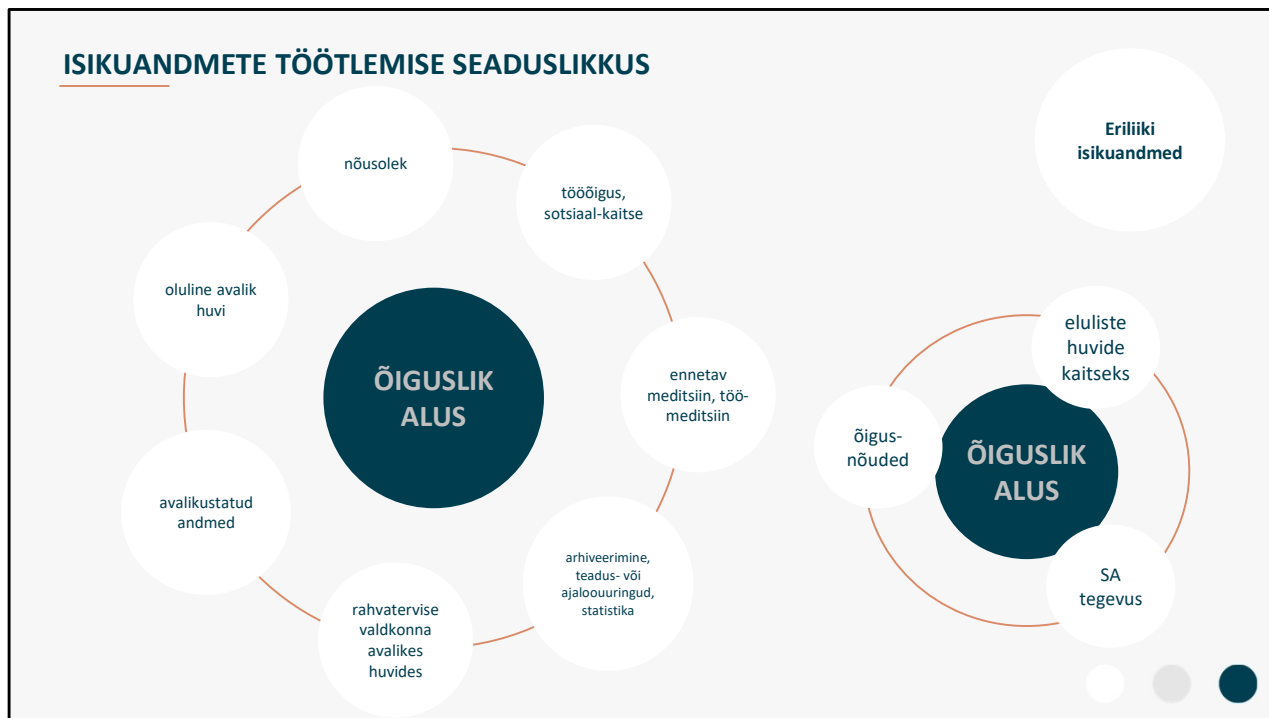


Andmekaitse Inspektsioon on koostanud detailse õigustatud huvi kaalumise juhendi (Kättesaadav:

[https://www.aki.ee/sites/default/files/dokumendid/oigustatud\\_huvi\\_juhend\\_15052020.pdf](https://www.aki.ee/sites/default/files/dokumendid/oigustatud_huvi_juhend_15052020.pdf)).

Järgides juhendis kajastatud põhimõtteid, peaks iga vastutav töötaja (enne isikuandmete töötlemist õigustatud huvi alusel) läbi viima kolmeastmelise kontrolli tuvastamiseks, kas töötlemise aluseks olev õigustatud huvi kaalub üles andmesubjekti huvid ja põhiõigused. Oluline on kogu kaalumisprotsess ka detailselt dokumenteerida, et täita ka IKÜM artikli 5 lõikes 2 sätestatud vastutuse põhimõtet. AKI on sageli ette heitnud, et andmesubjekti huve ja õigusi ei käsitleta piisavalt. Öeldakse lihtsalt üldsõnaliselt, et andmesubjektil on huvi privaatsusele. See ei ole piisav. Samuti tasub meeles pidada, et riik ei saa tõenäoliselt teadusuuringute jaoks tugineda õigustatud huvile.

Aitab, kui võimalikult selgelt piiritleda, mis on eesmärk ja milliseid andmeid selle eesmärgi täitmiseks on vaja. Koolituse käigus arutasime ka praktikast tulenenud näidet krediidiriski hindamiseks lekkinud andmebaaside kasutamisest (nt <https://haveibeenpwned.com/>). Ühest küljest aitab vältida pettusi (identiteedivargused), teisest küljest võib anda muud kasulikku sisendit, mida inimene ise ei tahaks anda, nt kui andmed on lekkinud hasartmängu lehtedelt.



Isikuandmete eriliikide töötlemine on IKÜM artikli 9 lõike 1 kohaselt keelatud. Erandina võib eriliiki isikuandmeid siiski töödelda, kui esineb mõni IKÜM artikli 9 lõikes 2 sätestatud eranditest. See ei tähenda, et artiklis 6 sätestatud õiguslikud alused võiks ära unustada. Pigem tuleb arvestada, et artikli 9 lõikes 2 sätestatud alused on lisareeglid artiklis 6 sätestatule.

Enamik tingimusi sõltub sellest, kas vastutav töötaja suudab tõendada, et eriliiki isikuandmete töötlemine on konkreetsel eesmärgil vajalik. See ei tähenda, et töötlemine peab olema absoluutselt hädavajalik. Kuid see põhjendus peab olema midagi enam kui lihtsalt “kasulik” või “harjumuspärane”. Isikuandmete eriliikide töötlemine on vajalik, kui see on sihipärane ja proportsionaalne viis selle konkreetse eesmärgi saavutamiseks.

Avalikus sektoris andmeanalüütika kontekstis isikuandmete eriliikide töötlemisest rääkides keskendume slaidi vasakul poolel esitatud alustele.



Isikuandmete eriliikide töötlemine ei ole keelatud, kui andmesubjekt on andnud selgesõnalise nõusoleku nende isikuandmete töötlemiseks ühel või mitmel konkreetsel eesmärgil, välja arvatud juhul, kui liidu või liikmesriigi õiguse kohaselt ei saa andmesubjekt IKÜM artikli 9 lõikes 1 nimetatud keeldu tühistada.

Selgesõnaline nõusolek tuleb kinnitada selge avaldusega (kas suuline või kirjalik), selline nõusolek ei saa olla kaudne.

Avaliku sektori puhul on nõusoleku alusel isikuandmete töötlemine võimupositsiooni tõttu küsitav. Peate olema kindel, et suudate näidata nõusoleku andmist vabatahtlikult.

Nõusoleku alusel – nt geenivaramu. Samas Geenivaramust saab andmeid konkreetse geenidoonori kohta ainult geenidoonor ise ja geenidoonori nõusolekul tema arst. Teadlased saavad vaid anonüümseid andmeid.

Nagu juba eespool märgitud – probleeme võib põhjustada nõusoleku tagasivõtmine.



Isikuandmete eriliikide töötlemine ei ole keelatud, kui töötlemine on vajalik seoses vastutava töötleja või andmesubjekti tööõigusest ning sotsiaalkindlustuse ja sotsiaalkaitse valdkonna õigusest tulenevate kohustuste ja eriõigustega niivõrd, kuivõrd see on lubatud liidu või liikmesriigi õigusega või liikmesriigi õiguse kohase kollektiivlepinguga, millega kehtestatakse asjakohased kaitsemeetmed andmesubjekti põhiõiguste ja huvide kaitseks.

See kehtib ka sotsiaalteenuste ja hüvitiste pakkumisega tegelevate riigiasutuste kohta. Sotsiaalkindlustus ja sotsiaalkaitse hõlmavad hüvitisi, sotsiaalset tuge või muid sekkumisi, mis on mõeldud inimeste abistamiseks. Kui töötlemine on seotud kitsalt tervishoiuga, siis võib olla asjakohasem järgmine alus.

Võimalike kaitsemeetmetena on IKÜM-is nimetatud võimalikult väheste andmete kogumist, anonüümimist ja andmeturvet. Kui teadusuuringute eesmärki on võimalik saavutada isikuandmeid töötlemata, on eelistatud lahendus anonüümimine.

Loe veel:

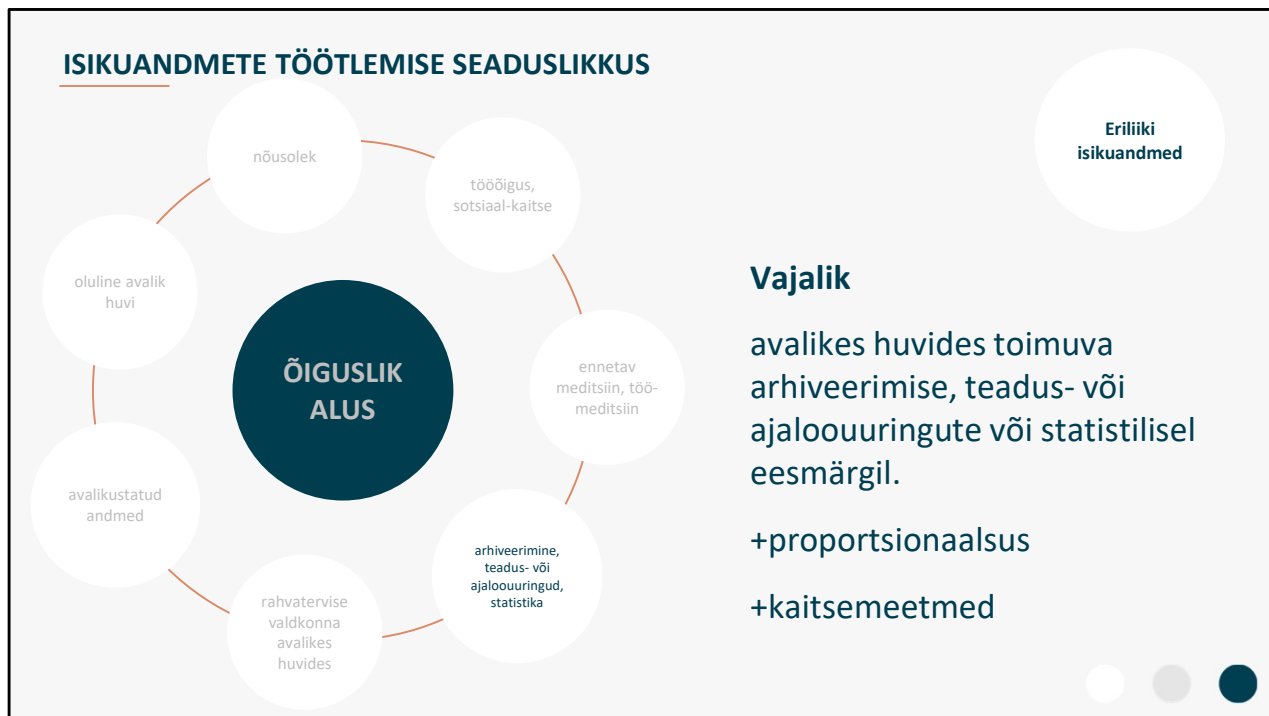
[https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_et.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_et.pdf)



Isikuandmete eriliikide töötlemine ei ole keelatud, kui töötlemine on vajalik ennetava meditsiini või töömeditsiiniga seotud põhjustel, töötaja töövõime hindamiseks, meditsiinilise diagnoosi panemiseks, tervishoiuteenuste või sotsiaalhoolekande või ravi võimaldamiseks või tervishoiu- või sotsiaalhoolekandesüsteemi ja -teenuste korraldamiseks, tuginedes liidu või liikmesriigi õigusele või tervishoiutöötajaga sõlmitud lepingule ja eeldusel, et IKÜM artikli 9 lõikes 3 osutatud tingimused on täidetud ja kaitsemeetmed kehtestatud.

See alus hõlmab näiteks tervishoiu või ravi pakkumisega seotud toiminguid, sotsiaalhoolekande pakkumisega seotud toiminguid (sh sotsiaaltöö, isikuhooldus ja sotsiaaltoetustega seonduvad toimingud) ning ka tervishoiusüsteemide või -teenuste või sotsiaalhooldussüsteemide või -teenuste haldamiseks vajalikke toiminguid.





Isikuandmete eriliikide töötlemine ei ole keelatud, kui töötlemine on vajalik avalikes huvides toimuva arhiveerimise, teadus- või ajaloouringute või statistilisel eesmärgil vastavalt IKÜM artikli 83 lõikele 1, tuginedes liidu või liikmesriigi õigusele, ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ning tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks.

Selliste toimingute puhul tuleb eraldi kaaluda nii toimingu proportsionaalsust kui ka rakendatavaid kaitsemeetmeid. Kuivõrd uuringute ja statistika jaoks ei ole sageli hädavajalik töödelda isikuandmeid (st isikustatud kujul andmeid), siis tuleb kaitsemeetmetega tagada nii tehniliste kui ka korralduslike meetmete olemasolu eelkõige selleks, et tagada võimalikult väheste andmete kogumise põhimõtte järgimine. Need meetmed võivad hõlmata pseudonümiseerimist, kui kõnealuseid eesmärke on võimalik saavutada sellisel viisil.

Nimetatud eesmärkidel isikuandmete töötlemisel tasub kindlasti vaadata ka IKS-is sätestatud siseriiklike sätteid.



Isikuandmete eriliikide töötlemine ei ole keelatud, kui töötlemine on vajalik rahvatervise valdkonna avalikes huvides, nagu kaitse suure piiriülese terviseohu korral või kõrgete kvaliteedi- ja ohutusnõuete tagamine tervishoiu ning ravimite või meditsiiniseadmete puhul, tuginedes liidu või liikmesriigi õigusele, millega nähakse ette sobivad ja konkreetsed meetmed andmesubjekti õiguste ja vabaduste kaitseks, eelkõige ametisaladuse hoidmine. See alus võib olla asjakohane näiteks andmete töötlemisel rahvatervise seireks ja statistika tegemiseks. Samuti on alus tõenäoliselt kohaldatav tervishoiusüsteemi ressursside planeerimiseks vajalike toimingute tegemiseks. Seoses koroonapandeemiaga võiks välja tuua näiteks isikuandmete töötlemise avalike vaksineerimisprogrammide teostamiseks.



Isikuandmete eriliikide töötlemine ei ole keelatud, kui töödeldakse isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud.

See tingimus ei hõlma kõiki üldkasutatavaid andmeid. See hõlmab ainult isikuandmeid, mille andmesubjekt ise on avalikustanud. Kui andmed on avalikuks saanud muul moel, siis ei ole sellel alusel isikuandmete eriliikide töötlemine lubatud (vaatamata sellele, et andmed on pealtnäha avalikud). Selle aluse valimisel peate olema kindel, et just isik ise otsustas aktiivselt oma eriliiki isikuandmed avalikustada ja et see pole olnud eksitus (sh kogemata liigsete andmete avaldamine). Eristada tuleb ka andmete avaldamiseks nõusoleku andmist või sellest teadlik olemist ning isiku aktiivset tegevust teabe kättesaadavaks tegemiseks.

Oluline on igakordselt sisustada ka avalikustamise kriteeriumi. Näiteks on Eestis kohtumõistmine avalik, kuid istungil avaldatu ei pruugi siiski olla üldsusele kättesaadav avalik teave. Seega ei pruugi olla võimalik kohtusaalis kohtunikule ja pooltele (sh nende lepingulistele esindajatele) avaldatud eriliiki isikuandmeid pidada ilmselgelt avalikustatud andmeteks.



Isikuandmete eriliikide töötlemine ei ole keelatud, kui töötlemine on vajalik olulise avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ja tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks. Sellel alusel võib eriliiki isikuandmete töötlemine kõne alla tulla näiteks riikliku julgeoleku eesmärkidel, terrorismi ja rahapesu tõkestamisel jne. Eestis ei ole kehtestatud selget nimekirja, mis on olulise avaliku huviga seotud põhjused, mis õigustaksid isikuandmete eriliikide töötlemist. Küllaga on selliseid nimekirju kehtestanud teiste riikide järelevalveasutused. Kuigi need ei ole Eestis kohalduvad, võib sellistest nimekirjadest olla kasu põhjenduste esitamisel ja sätte tõlgendamisel.



Kaasus isikuandmete määratlemise kohta.

**AUTOMAATNE TÖÖTLEMINE**

\*

**AUTOMATISEERITUD OTSUS**

\*

**PROFIILIANALÜÜS**



**MÕISTE**

**IKÜM artikkel 4 p 4**

**„Profiilanalüüs“ ...**

... igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab ...

... isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, ...

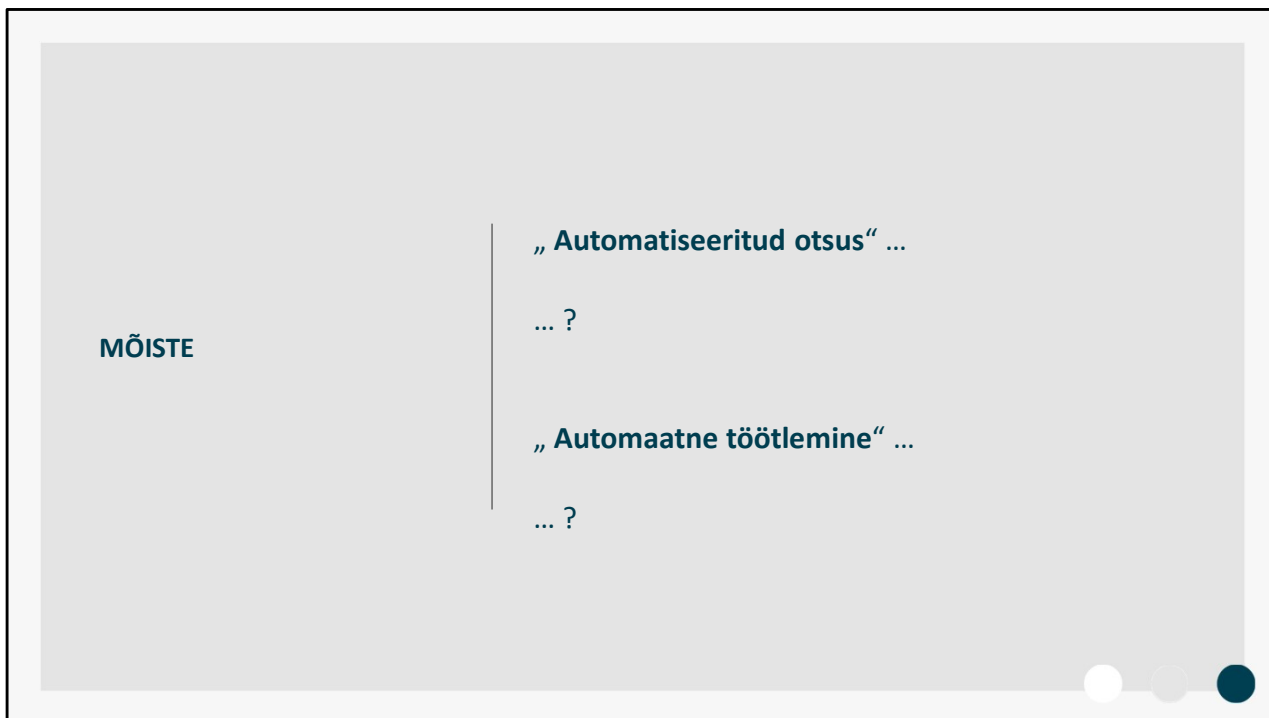
... eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud asjaomase füüsilise isiku:

- töötlemuste,
- majandusliku olukorra,
- tervise,
- isiklike eelistuste,
- huvide,
- usaldusväarsuse,
- käitumise,
- asukoha või liikumisega.

**Profiilanalüüs** on menetlus, mis võib hõlmata hulka statistilisi järeldusi. Seda kasutatakse sageli, et teha inimeste kohta prognoose, kasutades mitmesugustest allikatest pärit teavet, et järeldada üksikisiku kohta midagi, tuginedes statistiliselt sarnastena tunduvate teiste inimeste omadustele. (EDPB juhis). Oluline element HINDAMINE, ainult statistika ei loe.

Profiilanalüüsil on **kolm omadust**:

- tegemist peab olema automatiseeritud töötlemisega;
- seda tuleb teha isikuandmetega ning
- profiilanalüüsi eesmärk peab olema füüsilise isikuga seotud isiklike aspektide hindamine.



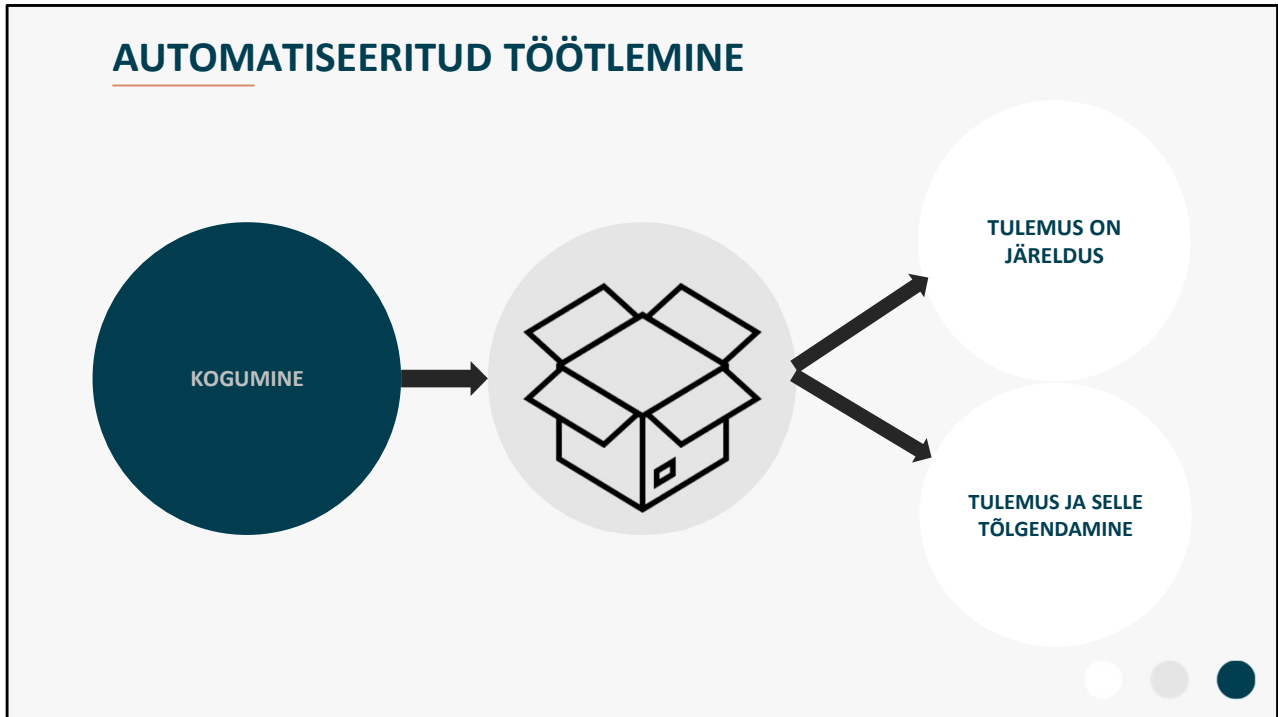
Automatiseeritud otsuste ja automaatse töötlemise kohta IKÜM-is täpseid mõisteid ei ole.

AKI kodulehel on automatiseeritud töötlusel põhinev otsus defineeritud kui otsus, mis tehakse infotehniliste vahenditega ja ilma inimese sekkumiseta (<https://www.aki.ee/et/eraelukaitse/automatiseeritud-otsused-ja-profiilianaluus>).

IKÜM art 35 ütleb mõjuhindangu kohta, et selle läbiviimine on kohustuslik kui toimub füüsiliste isiklike aspektide süstemaatiline ja ulatuslik hindamine, mis põhineb **automaatsel isikuandmete töötlemisel**, sealhulgas profiilianalüüs. International Association of Privacy Professionals (IAPP) kodulehel on automaatset töötlemist defineeritud järgnevalt: *A processing operation that is performed without any human intervention.*

Kuidas mõista automaatset töötlemist võrreldes digitaalse või elektroonilise töötlemisega? Tõlgendan nii, et „automaatne“ tähendab, et andmetega aktiivselt ja sisuliselt tehakse midagi. See ei ole lihtsalt digitaalne või elektrooniline säilitamine.





Automaatseid otsuseid saab teha koos profiilianalüüsiga või ilma selleta; profiilianalüüsi saab teha ilma automaatsete otsuste tegemiseta. Oluline inimsekkumise määr.

## AUTOMAATSED OTSUSED - ARTIKKEL 22

- Andmesubjektil on **õigus**, et tema kohta ei võetaks otsust, mis põhineb üksnes automatiseeritud töötlusel, sealhulgas profiilianalüüsil, mis toob kaasa teda puudutavaid õiguslikke tagajärgi või avaldab talle märkimisväärset mõju.
- käsitletav selliste otsuste tegemise **keeluna**, millest lubavad erandid

Niisiis tähendab automatiseeritud töötlemisel põhinev otsus, et inimene ei osale otsustusprotsessis. Et tegu oleks inimese sekkumisega, peab vastutav töötleja tagama, et otsuse läbivaatamine on mõtestatud, mitte üksnes tühi liigutus. Seda peaks tegema keegi, kellel on volitused ja pädevus otsust muuta. Ta peaks analüüsi käigus arvesse võtma kõiki asjakohaseid andmeid. Andmekaitsealases mõjuhinnangus peaks vastutav töötleja kindlaks tegema ja märkima inimese sekkumise taseme otsustusprotsessis ning selle, millises etapis sekkumine toimub.

Selles sättes kasutatav termin „õigus“ ei tähenda, et artikli 22 lõiget 1 kohaldataks üksnes siis, kui andmesubjekt õigust aktiivselt kasutab. Artikli 22 lõikes 1 on kehtestatud üksnes automatiseeritud töötlusel põhinevate otsuste tegemise üldine keeld. See keeld kehtib olenemata sellest, kas andmesubjekt võtab meetmeid seoses oma isikuandmete töötlemisega.

Nõutavad kaitsemeetmed hõlmavad õigust olla teavitatud (mida käsitletakse artiklites 13 ja 14 – täpsemalt sisuline teave kasutatava loogika kohta ning selle kohta, millised on töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks) ja kaitsemeetmeid nagu õigus otsesele isiklikule kontaktile ja õigus otsus vaidlustada (mida käsitletakse artikli 22 lõikes 3).

Iga töötlemise korral, mis kujutab endast andmesubjektile tõenäoliselt suurt ohtu, peab vastutav töötleja tegema andmekaitsealase mõjuhinnangu. Lisaks mistahes muude töötlemisega seotud ohtude käsitlemise võimaldamisele võib andmekaitsealane mõjuhinnang olla eriti kasulik vastutavatele töötlejatele, kes pole kindlad, kas nende kavandatav tegevus vastab artikli 22 lõikes 1 esitatud määratlusele, ning milliseid kaitsemeetmeid tuleb rakendada, kui töötlemine on kindlakstehtud erandi tõttu lubatud.

## ARTIKKEL 22 - ERANDID

- Automatiseeritud töötlusel põhinev otsus lubatud, kui:
  - vajalik lepingu täitmiseks või sõlmimiseks;
  - lubatud vastutava töötaja suhtes kohaldatava liidu või liikmesriigi õigusega, milles on sätestatud ka asjakohased meetmed andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks; või
  - põhineb andmesubjekti sõnaselgel nõusolekul.

P 1 või 3 peavad ka lisaks olema asjakohased kaitsemeetmed. Need meetmed peaksid hõlmama vähemalt viisi, kuidas andmesubjektil on võimalik saada otsene isiklik kontakt, väljendada oma seisukohta ja vaidlustada otsus.

## ARTIKKEL 22 - ERANDID

### § 33<sup>6</sup>. Automaatsed haldusaktid ja dokumendid ●

(1) Keskkonnaamet võib anda haldusakti ja dokumendi automatiseeritult, ilma maksuhalduri ametniku vahetu sekkumiseta (edaspidi *automaatne haldusakt ja dokument*), arvestades maksukorralduse seaduse § 46<sup>2</sup> lõikes 2 sätestatut. ○

### § 46<sup>2</sup>. Automaatsed haldusaktid ja dokumendid ●

(1) Riiklike maksude maksuhaldur võib anda haldusakti ja dokumendi automatiseeritult, ilma maksuhalduri ametniku vahetu sekkumiseta (edaspidi *automaatne haldusakt ja dokument*). ○

### § 23. Töötukassa eesmärk ●

(4) Töötukassal on oma eesmärgi saavutamiseks ja seaduses sätestatud ülesannete täitmiseks õigus anda haldusakte automatiseeritult isiku vahetu sekkumiseta, kui see on võimalik arvestades haldusakti andmise asjaolusid ja sisu.

[RT I, 13.03.2019, 2 - jõust. 15.03.2019] ●

### § 489<sup>2</sup>. Kohtunikuabi pädevus maksekäsu kiirmenetluses ja määruste tegemine automatiseeritult ●

(1) Maksete paneku, maksekäsu ja maksekäsu kiirmenetlusega seotud muu määruse, muu hulgas *käesoleva seadustiku §-s 179* nimetatud määruse, võib teha ka kohtunikuabi.

[RT I 2008, 28, 180 - jõust. 15.07.2008] ●

(2) Käesoleva paragrahvi lõikes 1 nimetatud määruse võib teha ka automatiseeritult maksekäsu kiirmenetluse infosüsteemi vahendusel, kui on tagatud määruse tegemise eelduste automaatne kontrollimine. Sel juhul ei pea määrus olema allkirjastatud.

[RT I, 21.05.2014, 1 - jõust. 31.05.2014] ●

Eestis on juba praegu mitmes õigusaktis näiteid automatiseeritud otsuste tegemise kohta. Esitatud näited on:

1. keskkonnatasude seaduse § 33.6 lg 1;
2. maksukorralduse seaduse § 46.2 lg 1;
3. töötuskindlustuse seaduse § 23 lg 4; ja
4. tsiviilkohtumenetluse seadustiku § 489.2.

## ARTIKKEL 22 – ERAND ERANDIST

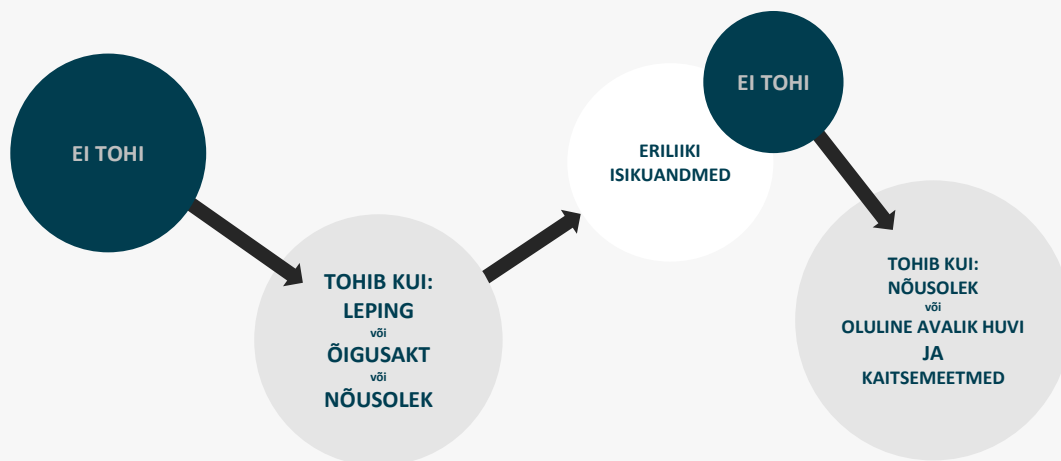
Eriliiki  
isikuandmed

- EI TOHI põhineda eriliiki isikuandmetel
- välja arvatud kui:
  - töötlemine nõusoleku alusel (art 9(2)(a)); või
  - vajalik olulise avaliku huviga seotud põhjustel (art 9(2)(g))
  - JA
  - kehtestatud on asjakohased kaitsemeetmed

Kui otsustamine hõlmab artikli 9 lõikes 1 määratletud andmete eriliike, peab vastutav töötleja ühtlasi tagama, et ta täidab artikli 22 lõikes 4 sätestatud nõudeid, st eriliikide töötlemise aluseks on nõusolek või oluline avalik huvi õigusaktis sätestatud alusel. Samuti peavad kindlasti olema kehtestatud asjakohased kaitsemeetmed.

## ARTIKKEL 22

Automatiseeritud töötlemisel põhinevad **otsused**



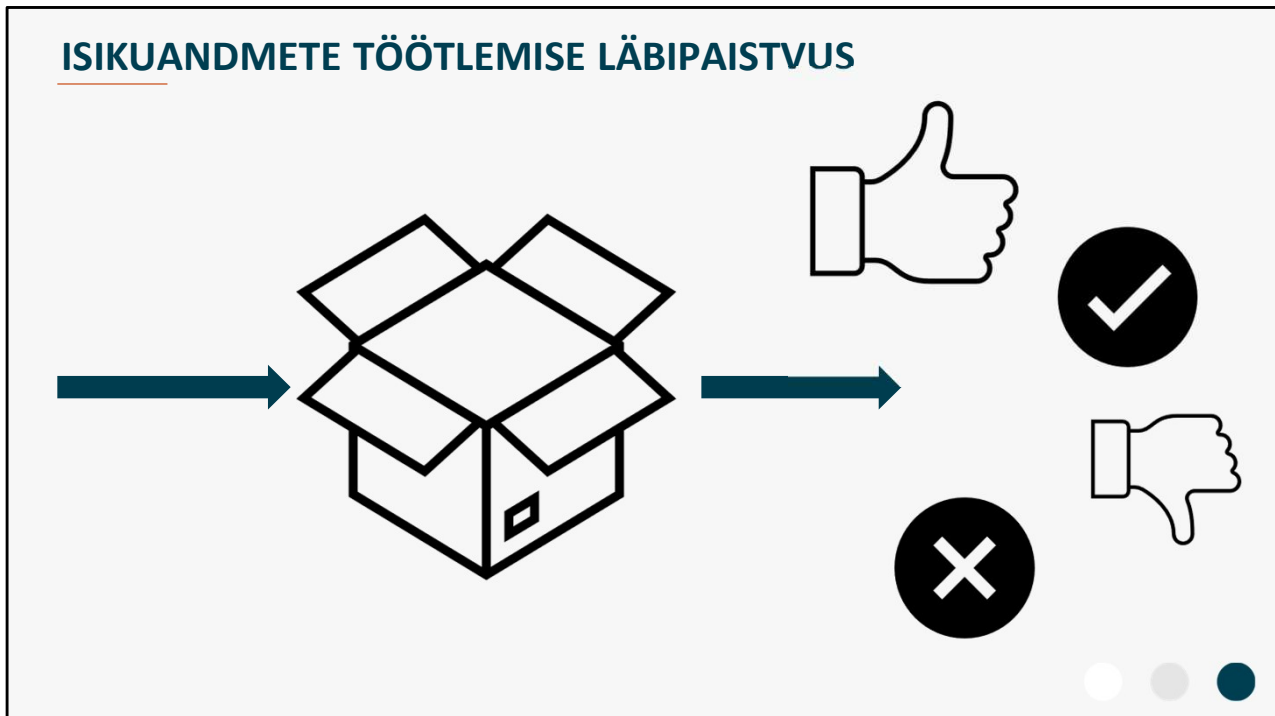
Kokkuvõtlik skeem automatiseeritud otsuste lubatavuse ja keeldude kohta.

**KÜSIMUS:** nt tahaks mõni mh järelevalvet teostav asutus teha manuaalse veebikammimise osas teha seda tööd andmekraapija alusel. Kui selle kogutud info alusel tehakse automaatselt ka mingi otsus, siis kohalduvad art 22 piirangud. Kui ainult kogutakse andmeid ja otsustusprotsessi sekkub inimene, siis automaatse otsustuse reeglid ei kohaldu. Küllaga võib tekkida mõjuhinnangu läbiviimise vajadus.

## ÜLDMÄÄRUS ARTIKKEL 12-14

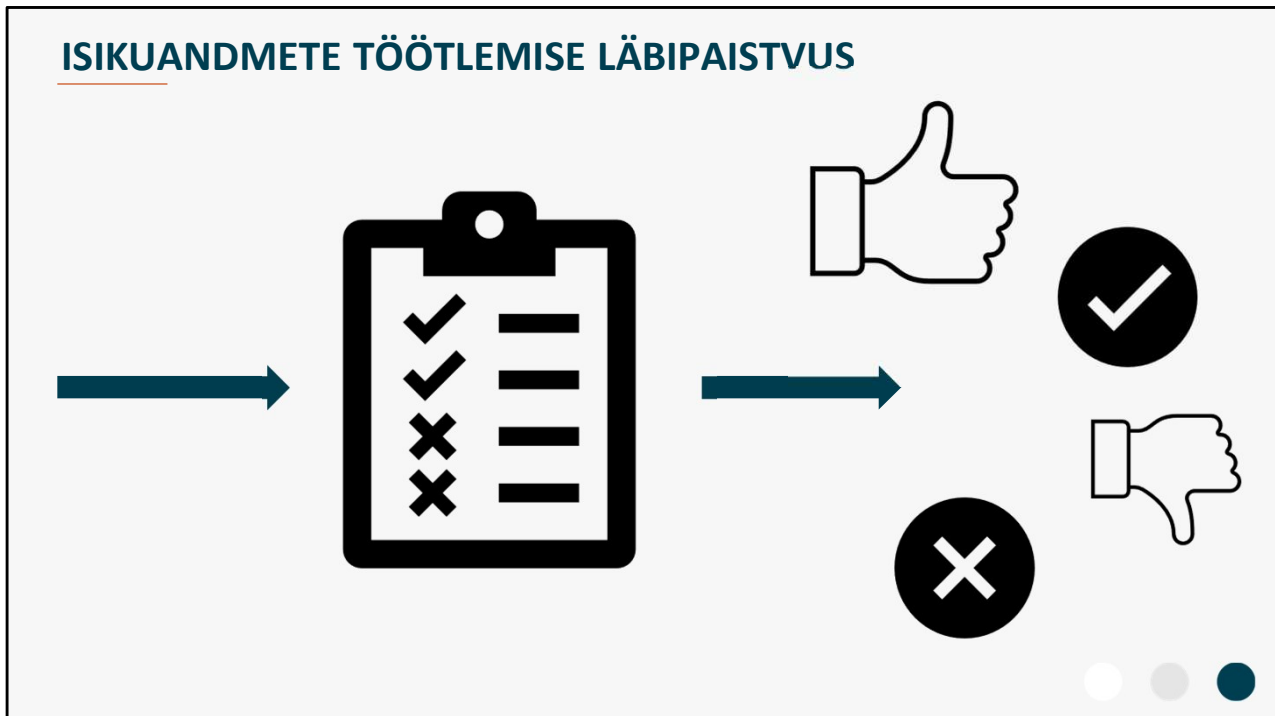
1. Kui andmesuutjega seotud isikuandmeid kogutakse andmesuutjalt, teeb vastutav töötleja isikuandmete saamise ajal andmesubjektile teatavaks kogu järgmise teabe:
- a) **Art 13 lg 2 p (f) ja art 14 lg 2 p (g):**
  - b) **teave [...] automatiseeritud otsuste, sealhulgas**
  - c) **profiilianalüüsi tegemise kohta ning vähemalt**
  - d) **nendel juhtudel sisuline teave kasutatava**
  - e) **loogika ja selle kohta, millised on sellise**
  - f) **töötlemise tähtsus ja prognoositavad tagajärjed**
  - g) **andmesubjekti jaoks.**
2. Peale andmesuutjaga seotud isikuandmete kogumise on vajalik õiguse ja läbipaistvuse tagamiseks:
- a) võimalik, sellise ajavahemiku määramise kriteeriumid;
  - b) teave õiguse kohta taotleda vastutavalt töötlejalt juurdepääsu andmesubjekti puudutavatele isikuandmetele ning nende parandamist või kustutamist või isikuandmete töötlemise piiramist või esitada vastuväide selliste isikuandmete töötlemisele, samuti teave isikuandmete ülekandmise õiguse kohta;
  - c) kui isikuandmete töötlemine põhineb artikli 6 lõike 1 punktil a või artikli 9 lõike 2 punktil a, siis teave õiguse kohta nõusolek igal ajal tagasi võtta, ilma et see mõjutaks enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust;
  - d) teave õiguse kohta esitada kaebus äärevalveasutusele;

Oluline probleem automatiseeritud otsuste puhul on andmesubjekti jaoks info edastamine ja läbipaistvuse tagamine. Andmeanalüütika kontekstis on läbipaistvuse põhimõtte puhul eriti oluline esitada andmesubjektile sisuline teave kasutatava loogika ja selle kohta, millised on sellise töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks.



Isikuandmete töötlemine ei tohiks üheski olukorras meenutada andmesubjektile “musta kasti”, mille puhul andmesubjekt ei saa aru, kas, kes, kuidas või miks tema isikuandmeid töötleb ning milliseid järeltusi kogutud andmetest tehakse. Aga sageli tänapäeva TI (AI) süsteemide puhul ei saa selle looja isegi enam aru, millel ja kuidas järeltused täpselt põhinevad.





Peaks olema selge vähemalt üldine toimimise loogika. Peavad olema olemas ka vajalikud load. Väikese kõrvalepõikena tuletame meelde, millal lubasid vaja:

**AKI luba** on vaja taotleda, kui asutus viib läbi poliitikakujundamise uuringu ning selleks tehakse päringuid teise vastutava või volitatud töötaja andmekogusse või kasutatakse teise vastutava või volitatud töötaja vastutusalas olevaid andmete kogumeid. Kui poliitikakujundamise uuring viiakse läbi eriliigiliste isikuandmetega, peab olema enne AKI-lt loa taotlemist saadud luba eetikakomiteelt. Luba on vaja taotleda ka siis, kui eriliigilisi isikuandmeid sisaldav uuring viiakse läbi teadusvaldkonnas, kus puudub eetikakomitee. Tavapäraste isikuandmetega tehtavad uuringud ei vaja AKI luba.

**Luba ei ole vaja** taotleda, kui isikuandmeid töödeldakse teadusuuringus isiku nõusolekul. Kuid sellisel juhul rakendub isikuandmete töötlemisele üldine andmekaitse regulatsioon. Luba ei ole vaja taotleda ka siis, kui teadusuuring viiakse läbi anonüümsete andmetega

Loe veel: <https://www.aki.ee/et/eraelu-kaitse/isikuandmed-uuringutes>

Eestis on nt: Bioeetika ja Inimuuringute Nõukogu, Tervise Arengu Instituudi inimuuringute eetikakomitee, Ülikoolide juures tegutsevad eetikakomiteed (TTÜ eetikakomitee, Tartu Ülikooli inimuuringute eetika komitee, Tallinna Ülikooli eetikakomitee), Organisatsioonipõhised eetikakomiteed (Eesti Arstide Liidu eetikakomitee, Tallinna Lastehaigla eetikakomitee, Tartu Ülikooli Kliinikumi eetikakomitee, Põhja-Eesti Regionaalhaigla eetikanõukogu).



## ÕIGLUS JA LÄBIPAISTVUS

- teave ja sõnumid on lihtsalt kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud
- töötleja identiteet ja töötlemise eesmärgid
- õiguste ja kaitsemeetmete olemasolu ning nende kasutamine

Andmesubjektile peab läbipaistvuse huvides andma selgelt ka infot, kes on tema isikuandmete vastutav töötaja. Teave on andmesubjektile oluline, et teada, kelle poole pöörduda küsimuste, taotluste ja nõuetega. See kohustus seondub tihedalt kohustusega esitada andmesubjektile teave tema õiguste ja nende kasutamise kohta. Andmesubjekti õigustest on koolituses juttu edaspidi. Samuti peab andmesubjekti teavitama isikuandmete vastuvõtjatest (sh volitatud töötajatest), kellele isikuandmeid on edastatud või plaanitakse edastada.

## Facebook – Cambridge Analytica skandaal

- USA 2016. aasta presidendivalimiste ajal.
- kampaaniameeskonna palgatud andmeanalüüsifirma Cambridge Analytica kasutas 50 miljonilt Facebooki kasutaja profiililt andmeid, et luua tarkvara valijate valikute prognoosimiseks ja **mõjutamiseks**.
- Briti informatsioonikomisjon (ICO) uurimine näitas, et Facebook käitles vahemikus 2007-2014 kasutajate andmeid ebaõiglaselt, edastades neid rakenduste arendajatele selleks nõusolekut küsimata.
- ICO määras 2018. aastal Facebookile trahvi 565 300 eurot.

<https://www.err.ee/871909/facebook-sai-cambridge-analytica-skandaali-ees-50-miljonit-naela-trahvi>

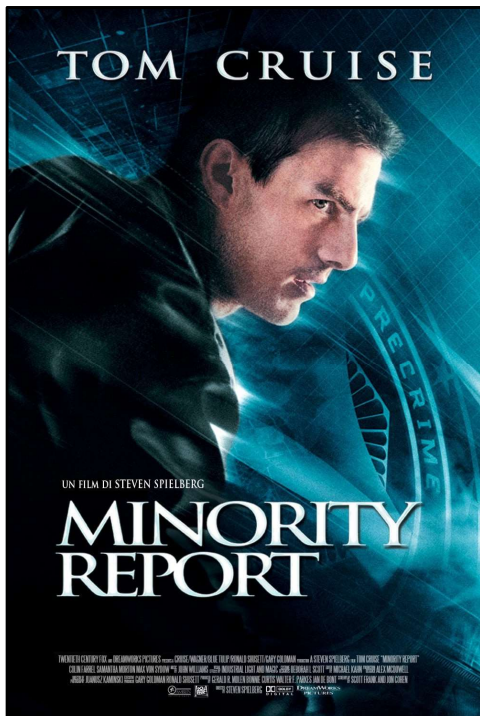
Läbipaistmatu andmetötluse riskid on nii rahulolematu andmesubjekt, inimeste usalduse kaotus kui ka trahvid. ICO tehtud trahv tundub praeguseks küll väike, kuid see oli maksimaalne lubatud trahv rikkumise ajal.

Enne kui on võimalik Facebooki meeldimiste (*like*) abil inimese psühholoogilist profiili ennustada, peab ca paarsada tuhat inimest tegema 120-küsimusega isiksuseviktoriini (ühe standardse psühholoogilise uuringu lühiversiooni pikkus). "Treeningukomplekt" viitab nendele andmetele tervikuna: Facebooki meeldimised, isiksusetestid ja kõik muu, millest sooviti õppida. Teises otsas on vaja "sihtmootajaid" ehk asju, mida prooviti ennustada. Konkreetse näite puhul isiksuseomadusi või poliitilist orientatsiooni.

Uuringu kasutaja jaoks oli protsess kiire: kasutaja klõpsas rakendusel ja sai mingi boonuse. Kuid nende paari sekundi jooksul juhtus kaks väga olulist asja. Esiteks kogus rakendus äsja sisse loginud kasutaja kohta võimalikult palju andmeid (sh isikut tuvastavat teavet, nagu pärisnimi, asukoht ja kontaktandmed – midagi, mida ei olnud küsitlussaitide endi kaudu võimalik sisestada). Teiseks tegi rakendus sama asja kõigi selle kasutaja sõpradega.

Algoritmid ühendasid andmed teiste allikatega, näiteks hääletajate kirjetega, et luua suurepärane kirjete kogum (alguses 2 miljonit inimest 11 põhiosariigis), mis sisaldab sadu andmepunkte inimese kohta. Neid inimesi sai seejärel sihtida nende isikuandmete põhjal väga isikupärastatud reklaamidega

Loe veel: <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>. Samal teemal dokumentaalfilm „The Great Hack“ (2019).



2002

### Steven Spielbergi film

The year is 2054. Murders can be now be stopped before they even occur, thanks to the sophisticated techniques of the PreCrime police unit, ...

Film „Minority Report“ tundus 2002. aastal tõelise ulmepõnevikuna, kuid juba 2014 kasutas Chicago politsei tehisintellektil põhinevat analüüsi, et külastada isikuid, kelle puhul süsteem teavitab võimalikust seosest vägivallakuritegudega tulevikus.

Justiitsministeeriumi väljatöötamiskavatsus seoses krattide reguleerimisega: Eestis puudub korrakaitseaduses ohuennetuse ja võimalike rikkujate tuvastamise eesmärgil andmekogude andmete kasutamist reguleeriv säte, mis annaks aluse ja raamid ohuennetuse eesmärgil toimuvale massandmetöötlusele. Proaktiivsete teenuste arendamisel tehisintellekti poolt kõigi inimeste profileerimisel (inimeste kavatsuste tuvastamisel) tekib tõsine põhiseaduslik probleem inimväärikuse ja eraelu puutumatusse riive kontekstis (<https://www.kratid.ee/>, VTK lk 15).

Vaatamata oma innovatsioonipotentsiaalile võivad suurandmed kujutada endast olulisi riske isikuandmete kaitsele ja eraelu puutumatusse. Eelkõige tekitavad muret andmete kogumise, jälgimise ja profiilide koostamise tohutu ulatus, võttes arvesse ka kogutud andmete mitmekesisust ja üksikasjalikkust ning asjaolu, et andmeid kombineeritakse sageli paljudest erinevatest allikatest. Seejuures jäävad kaitsetasemed sageli tagaplaanile. Tagajärjeks on süsteemi ebatäpsus, diskrimineerimine, tõrjutus ja majanduslik tasakaalustamatus.

Tehisintellekti määruse eelnõus järgitakse riskipõhist lähenemisviisi, eristades tehisintellekti kasutusviise, mis tekitavad i) vastuvõetamatu riski, ii) suure riski ja iii) väikese või minimaalse riski. Näiteks on eelnõus selgelt keelatud ametiasutuste kasutatav tehisintellektipõhine sotsiaalne hindamine üldistel eesmärkidel. Keelustatakse ka reaajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse eesmärgil avalikult juurdepääsetavates ruumides, välja arvatud juhul, kui kohaldatakse teatavaid piiratud erandeid.

## TEHNILISED JA KORRALDUSLIKUD MEETMED

- Füüsiliste isikute õiguste ja vabaduste kaitsmine isikuandmete töötlemisel eeldab asjakohaste **tehniliste ja korralduslike meetmete** kasutusele võtmist.
- Tehniliste ja korralduslike meetmete rakendamise eesmärk on IKÜM-is sätestatud põhimõtete (kohustuste) täitmine:
  - seaduslikkus, õiglus ja läbipaistvus;
  - eesmärgi piirang;
  - võimalikult väheste andmete kogumine;
  - õigsus;
  - säilitamise piirang;
  - usaldusvärsus ja konfidentsiaalsus.

Selleks, et isikuandmed oleks korrektselt kaitstud, peab vastutav töötleja kohaldama asjakohaseid tehnilisi ja korralduslikke meetmeid.

## KORRALDUSLIKUD MEETMED

Sise-eeskirjad ja muud seotud küsimused, näiteks:

- vastutavad isikud/positsioonid;
- olulise informatsiooni koordineerimine;
- juurdepääs andmetele, ruumidele või seadmetele;
- talitluspidevuse kokkulepped;
- perioodilised kontrollid ja auditid.

Määrus ei loetle otseselt, mis on kohustuslikud korralduslikud meetmed. Siiski annab IKÜM selle kohta mõningaid vihjeid. Näiteks põhjendus p 78 sätestab, et vastutav töötleja peaks võtma vastu sise-eeskirjad, et olla võimeline tõendama määruse täitmist,.

Sise-eeskirjade kehtestamine on oluline ka info jagamiseks. Näiteks, et oleks selge, kellele tuleb infot anda uute protsesside kasutusele võtmisest või uute seadmete süsteemi liitmisest. Läbi tuleb mõelda talitluspidevuse kokkulepped - kuidas te kaitsete ja taastate mis tahes teie valduses olevaid isikuandmeid?

Millised sise-eeskirjad olema peaks? Need peaks kirjeldama olulisi protsesse, jäädes samas selgeks, lühikeseks ja arusaadavaks. Protsesside kirjelduste üles tähendamine aitab neid ka läbi mõelda. Lühikeste sisukate dokumentide koostamine on keeruline, aga aitab teistel protsesse mõista ja aitab endal õigeid küsimusi küsida.

## TEHNILISED MEETMED

- IKÜM artikkel 32 – töötlemise turvalisus
- isikuandmete **pseudonümiseerimine** ja **krüpteerimine**;
- võime tagada isikuandmeid töötlevate süsteemide ja teenuste kestev **konfidentsiaalsus, terviklus, kättesaadavus** ja **vastupidavus**;
- **võime taastada** õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi korral;
- tehniliste ja korralduslike meetmete tõhususe **korrapärase testimise ja hindamise kord** isikuandmete töötlemise turvalisuse tagamiseks.

IKÜM artikkel 32 sätestab, et tehnilised meetmed hõlmavad MUU HULGAS järgmist (vt slaidil), st tegemist on näidete, mitte ammendava loeteluga.



**KAALUTLUSED**

**IKÜM artikkel 32 lg 1**

Võttes arvesse ...

- ... teaduse ja tehnoloogia viimast **arengut** ja ...
- ... rakendamise **kulusid** ning ...
- ... arvestades isikuandmete **töötlemise** laadi, ulatust, konteksti ja eesmäärke, ...
- ... samuti erineva tõenäosuse ja suurusega **ohte [riske]** füüsiliste isikute õigustele ja vabadustele, ...
- ... rakendavad vastutav töötleja ja volitatud töötleja ohule [riskile] vastava turvalisuse taseme tagamiseks **asjakohaseid** tehnilisi ja korralduslikke meetmeid

Oht = mis võib juhtuda. IKÜM eesti keelses tõlkes kasutatakse kohati sõna „risk“ asemel sõna „oh“, mis võib olla mõnevõrra eksitav. Tasub paralleelselt vaadata erinevate keelte tõlkeid.

Peaks keskenduma konkreetsetele vahenditele, mida võidakse kasutada nt anonüümimistehnika tagasipööramiseks, seda eeskätt seoses selliste vahendite rakendamiseks vajalike kulude ja oskusteabega ning tagasipööramise tõenäosuse ja raskusastme hindamisega.

## **PRIVAATSUST SÄILITAVAD TEHNOLOOGIAD**

*Privacy-enhancing technologies (PET)*

- Pseudonümiseerimine
- Turvaline ühisarvutus (kahe- või mitmepoolne)
- Anonümiseerimine
  - Juhuslikustamine:
    - Müra lisamine
    - Ümberjärjestamine
    - Diferentsiaalprivaatsus
  - Üldistamine:
    - k-anonüümsus
    - I-hajutus
    - t-lähedus
- Sünteetilised andmed

Miks see andmekaitse mõttes hea on? Aitab kaitsta andmesubjekti. Samas tuleb meeles pidada, et tegemist on üldjuhul isikuandmete töötlemise toiminguga, milleks peab olema õiguslik alus. Esimene eeltingimus see, et isikuandmed peavad senini olema kogutud ja töödeldud kooskõlas õigusaktidega. Anonüümimisprotsess vms muu on täiendav toiming.

## **PRIVAATSUST SÄILITAVAD TEHNOLOOGIAD**

*Privacy-enhancing technologies (PET)*

### ● **Pseudonümiseerimine**

- Turvaline ühisarvutus (kahe- või mitmepoolne)

### ● Anonümiseerimine

Juhuslikustamine:

- Müra lisamine
- Ümberjärjestamine
- Diferentsiaalprivaatsus

Üldistamine:

- k-anonüümsus
- I-hajutus
- t-lähedus

- Sünteetilised andmed



**Pseudonümiseerimine** – võimaldab võrreldes nt anonümiseerimisega säilitada rohkem andmeid. Samuti võimaldab pärast info uuesti isikuga kokku viia. Nt mingi ravimi statistika puhul võib olla pärast vaja info ka patsiendile edasi anda. Pseudonüümimine võimaldab tõenäoliselt tuvastamist ning kuulub seetõttu andmekaitsealaste õigusaktide reguleerimisalasse. Pseudonüümimine vähendab andmekogumi seostatavust andmesubjekti algse isikuga ning on seepärast kasulik turvameede, kuid mitte anonüümimismeetod.

Pseudonüümimise tulemus võib olla algsest väärtusest sõltumatu (nagu vastutava töötleja loodud juhusliku hulga või andmesubjekti valitud perekonnanime puhul) või tuletatav atribuudi või atribuutide kogumi algväärtustest (räsifunktsioon või krüpteerimine). Tehnikad näiteks:

- salavõtmega krüpteerimine;
- erinevad räsifunktsioonid (hea kasutada nt andmestike võrdlemiseks) – räsise soolamine, talletatud võtmega arvutatud räsi;
- tokeniseerimine – kasutatakse palju finantssektoris.

Palju tehnilisi riske. Nt ei tasu kasutada sama võtit erinevates andmebaasides (võimaldab seostada) või erinevaid võtmeid erinevate kasutajarühmade puhul (joonistuvad mustrid). Samuti tuleb mõelda, kuidas tagada pseudonümiseeritud andmete ja „võtme“ eraldi (+turvaline) talletamine.

Hea kasutada näiteks pilveteenusest tulenevate riskide maandamiseks – pilves ainult pseudonümiseeritud andmed, võtmed enda käes. Samas tasub meeles pidada nõ kaudselt lisatavaid andmeid – nt kui on tegemist KOV uuringuga, siis isegi kui aadressid kustutada, on kaudselt lihtne eeldada, et isiku elukoht on KOV piires.

## **PRIVAATSUST SÄILITAVAD TEHNOLOOGIAD**

*Privacy-enhancing technologies (PET)*

● Pseudonümiseerimine

● **Turvaline ühisarvutus (kahe- või mitmepoolne)**

● Anonümiseerimine

Juhuslikustamine:

● Müra lisamine

● Ümberjärjestamine

● Diferentsiaalprivaatsus

Üldistamine:

● k-anonüümsus

● l-hajutus

● t-lähedus

● Sünteetilised andmed



Turvalise ühisarvutuse abil saavad osapooled teha arvutusi nii, et iga osapool saab teada ainult arvutuse tulemuse ja ei saa teada midagi uut lähteandmete kohta. Turvaline ühisarvutus on krüptograafiline lahendus. Samas - ühissalastatud andmete peal töötamine aeglasem kui salastamata andmete peal.

Loe veel: <https://dspace.ut.ee/handle/10062/32994?locale-attribute=et>, <https://www.sirp.ee/s1-artiklid/c21-teadus/privaatsust-sailitav-andmeanaluus/>.

## PRIVAATSUST SÄILITAVAD TEHNOLOOGIAD

*Privacy-enhancing technologies (PET)*

- Pseudonümiseerimine
- Turvaline ühisarvutus (kahe- või mitmepoolne)

### ● Anonümiseerimine

Juhuslikustamine:

- Müra lisamine
- Ümberjärjestamine
- Diferentsiaalprivaatsus

Üldistamine:

- k-anonüümsus
- l-hajutus
- t-lähedus

- Sünteetilised andmed

Üldjuhul võrdväärne kustutamisega. See aitab täita andmete minimaalse säilitamise põhimõtet. Samas uuringutest nähtub, et täielikult anonüümse andmekogumi saamine rikkalikust isikuandmete hulgast nii, et alles jääb enamik otstarbekohasest olulisest teabest, ei ole kerge. Näiteks võib anonüümseks peetavat andmekogumit kombineerida mõne muu andmekogumiga viisil, mille tulemusel on üks või mitu isikut tuvastatavad. Lisaks oluline meeles pidada, et andmed kvalifitseeruvad kõigi osaliste jaoks endiselt kui isikuandmed seni, kuni vastutaval töötlejal (või muul osalejal) on juurdepääs algsetele toorandmetele.

Peamised anonüümsuse piisavusega seotud riskid on:

- **Eristatavus**, s.o võimalus eristada ühe või mitu andmesisendit, mille kaudu saab tuvastada üksikisiku andmekogumit.
- **Seostatavus**, s.o võimalus seostada omavahel vähemalt kahte andmesisendit ühe andmesubjekti või andmesubjektide rühma kohta (sama andmebaasi või eri andmebaaside lõikes). Kui ründaja suudab (näiteks korrelatsioonianalüüsi teel) tuvastada, et samale isikute rühmale kuulub kaks andmesisendit, kuid ei suuda eristada rühmast üksikisikuid, siis pakub tehnika kindluse eristatavuse, kuid mitte seostatavuse vastu.
- **Tuletatavus**, s.o võimalus tuletada suure tõenäosusega atribuudi väärtus muude atribuutide kogumis sisalduvatest väärtustest.

Kasutatakse juhuslikustamise ja üldistamise tehnikaid.

Loe veel: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_et.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_et.pdf) lk 11-12 .

## **PRIVAATSUST SÄILITAVAD TEHNOLOOGIAD**

*Privacy-enhancing technologies (PET)*

- Pseudonümiseerimine
- Turvaline ühisarvutus (kahe- või mitmepoolne)

- Anonümiseerimine

Juhuslikustamine:

- Müra lisamine
- Ümberjärjestamine
- Diferentsiaalprivaatsus

Üldistamine:

- k-anonüümsus
- I-hajutus
- t-lähedus

- **Sünteesilised andmed**

Sünteesiliselt genereeritud andmed koosnevad täiesti uutest ja kunstlikest andmepunktidest, millel pole üks-ühele seost algandmetega.

**Näilikud andmed** – juhuslikult genereeritud, ei sarnane pigem „päris“ andmetega.

**Reeglipõhised andmed** – genereeritud eelnevalt määratletud reeglistikuga. Andmete kvaliteet sama hea kui eelnevalt määratletud reeglistik. See toob kaasa väljakutseid, kui kõrge andmekvaliteet on esmatähtis.

**TI (AI) loodud andmed** – tehisintellekti mudelit koolitatakse algandmete põhjal, et õppida tundma kõiki omadusi, seoseid ja statistilisi mustreid. Seejärel suudab see TI-algoritm genereerida täiesti uusi andmepunkte ja modelleerida neid uusi andmepunkte nii, et see reprodutseerib algse andmestiku omadused, seosed ja statistilised mustrid. Kõige sarnasem „päris“ andmetega.

## ANDMEKAITSEALANE MÕJUHINNANG

- võtta arvesse
  - isikuandmete töötlemise laadi
  - ulatust
  - konteksti
  - eesmärke
  - kasutatav tehnoloogia (eriti, kui kasutatakse uut tehnoloogiat)
- kui tekib tõenäoliselt suur oht füüsilise isiku õigustele ja vabadustele
- vaja läbi viia **enne töötlemist** ja **värskendada** vastavalt vajadusele

Kui teatavat tüüpi isikuandmete töötlemise, eelkõige uut tehnoloogiat kasutava töötlemise tulemusena ning isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht, hindab vastutav töötleja enne isikuandmete töötlemist kavandatavate isikuandmete töötlemise toimingute mõju isikuandmete kaitsele. Endast sarnast suurt ohtu kujutavaid sarnaseid isikuandmete töötlemise toiminguid võib hinnata koos. Viide andmesubjektide õigustele ja vabadustele hõlmab eeskätt õigust isikuandmete kaitsele ja eraelu puutumatusse, kuid võib hõlmata ka muid põhiõigusi, nagu sõnavabadus, mõttevabadus, liikumisvabadus, diskrimineerimiskeeld, õigus vabadusele ning südametunnistuse- ja usuvabadus. AKI hinnangul on suure ohuga tegemist nt kui töödeldakse terviseandmeid haiglates ja tervisekeskustes või toimub isikuandmete edastamine välisriikidesse.

Mõjuhinnangut tuleks vaadelda kui abivahendit andmeanalüütika toimingute tegemisel. Mõjuhinnangu läbi viimine võib olla väga kasulik näiteks selleks, et põhjendada isikuandmete töötlemise vajalikkust. Kindlasti aitab see protsess leida tasakaalu ka isikuandmete minimaalsuse põhimõttega seoses. Mõjuhinnang aitab välja selgitada, millised andmed on vajalikud, et ei kogutaks liiga palju ega liiga vähe andmeid. Mõlema äärmusega kaasnevad andmeanalüütika puhul olulised riskid, mida mõjuhinnangu tegemisel eelduslikult märgatakse ja neid siis vastavalt maandatakse.

## ANDMEKAITSEALANE MÕJUHINNANG

- võtta arvesse
  - isikuandmete töötlemise laadi
  - ulatust
  - konteksti
  - eesmärke
  - kasutatav tehnoloogia (eriti, kui kasutatakse uut tehnoloogiat)
- kui tekib tõenäoliselt suur oht füüsilise isiku õigustele ja vabadustele
- vaja läbi viia **enne töötlemist** ja **värskendada** vastavalt vajadusele

Andmekaitsealane mõju hindamine ei ole ühekordne tegevus. Kui andmetöötluse käigus ilmnevad uued suured ohud, siis tuleks mõjuhindangut uuendada. Andmekaitsealane mõjuhindang aitab saavutada isikuandmete töötlemise toimingute vastavust IKÜM nõuetele ja seda ka tõendada.

Avalikus sektoris andmete töötlemisel tasub meeles pidada, et kui isikuandmete töötlemine toimub õigusakti alusel, siis võib mõjuhindang olla läbi viidud juba ka akti eelnõu raames (IKÜM artikli 35 lg 10). Võiks isegi väita, et põhjaliku mõjuhindangu läbi viimine õigusakti välja töötamise eelnõu raames on tungivalt soovituslik. Ebaotstarbekas oleks kehtestada õigusakt, mille rakendamise käigus selguvad alles suuremad probleemid isikuandmete töötlemise küsimustes.



## ANDMEKAITSEALANE MÕJUHINNANG

AKI aastaraamat 2020:

- Samuti kipuvad andmekaitsealased mõjuhinnangud kas **puuduma** või olema samuti **napisõnalised**.
- Sestap on tulnud mitmel korral tähelepanu juhtida vajadusele just andmekaitsealast **mõjuhinnangut täiendada**.
- **Mõju inimeste privaatsusele** kiputakse hindama ka pigem väiksemaks, kui see inspeksiooni hinnangul tihtipeale on.

Andmekaitse Inspeksioon on 2020 kokkuvõttes järeldanud, et andmekaitsealased mõjuhinnangud kipuvad kas puuduma või olema napisõnalised. Sestap on tulnud mitmel korral tähelepanu juhtida vajadusele just andmekaitsealast mõjuhinnangut täiendada. Mõju inimeste privaatsusele kiputakse hindama ka pigem väiksemaks, kui see inspeksiooni hinnangul tihtipeale on. Kuigi privaatsus ei ole absoluutne õigus, tasub seda mõjuhinnangu tegemisel pigem selle nurga alt vaadelda.

Praktilise soovitusena on eluliselt alati hea mõelda oma andmetele. Kas mõjuhinnangu läbiviija tahaks, et tema andmeid kirjeldatud viisil töödeldakse.

## ANDMEKAITSEALANE MÕJUHINNANG

- Kohustuslik läbi viia KUI:
  - automaatsel töötlemisel põhinev isiklike aspektide **süsteemaatiline ja ulatuslik hindamine**, mille põhjal tehakse otsuseid, millel on füüsilise isiku jaoks **olulised tagajärjed**
  - Isikuandmete **eriliikide** või süüdimõistvate kohtuotsuste ja süütegudega seotud andmete **ulatuslik töötlemine**, või
  - avalike alade ulatuslik süsteemaatiline jälgimine

Teatud eelduste puhul on mõjuhinnangu läbiviimine kohustuslik. IKÜM artikli 35 lõikes 3 on esitatud näited, millal on mõjuhinnangu läbi viimine kindlasti kohustuslik. Oluline on meeles pidada, et need on näited ja tegemist ei ole ammendava loeteluga.

Õiguskirjanduse kohaselt tasub "suure ohu" hindamisel lähtuda näiteks järgmistest elementidest (kui on täidetud vähemalt kaks kriteeriumi, oleks suure tõenäosusega vaja läbi viia andmekaitsealane mõjuhinnang):

1. Hindamine, sealhulgas profiilianalüüsi tegemine ja prognoosimine;
2. Õiguslike või samaväärsete oluliste tagajärgedega automatiseeritud otsuste tegemine;
3. Süsteemaatiline jälgimine;
4. Tundlikud andmed või väga isiklikud andmed;
5. Isikuandmete ulatuslik töötlemine;
6. Andmekogumite sobitamine või kombineerimine;
7. Haavatavate andmesubjektide andmed;
8. Uuenduslik kasutamine või uute tehnoloogiliste või korralduslike lahenduste rakendamine;
9. Kui isikuandmete töötlemise toimingud ise „takistavad andmesubjektidel õiguse või teenuse või lepingu kasutamist“.

## ANDMEKAITSEALANE MÕJUHINNANG

- automatiseeritud andmetöötlus
- ulatuslik töötlemine
- süstemaatiline töötlemine
- andmesubjektile tekivad õiguslikud tagajärjed või on muu oluline mõju

Vaatleme andmeanalüütika kontekstis lähemalt IKÜM artikli 35 lõike 3 punktis a kirjeldatud juhtu mõjuhinnangu läbiviimiseks.

## SÜSTEMAATILINE JA ULATUSLIK

- SÜSTEMAATILINE

- planeeritud ja metoodiline

- ULATUSLIK

- eriliiki andmed vähemalt 5000 inimese kohta
- suurt ohtu põhjustavaid andmed vähemalt 10 000 inimese kohta
- ülejäänud isikuandmed vähemalt 50 000 inimese kohta

erandid piiriülese andmetöötuse puhul

Suurt ohtu põhjustavad andmed (“ulatuslikkuse” kriteeriumi punkt 2) on nn tundlikud isikuandmed. Eestis on Andmekaitse Inspeksioon suurt ohtu põhjustavate andmetena nimetanud andmeid, millega võib kaasneda:

1. identiteedivarguse või -pettuse oht (eriti digitaalse usaldusteenuse ning sellega võrreldava identiteedihaldusteenuse puhul);
2. oht varale (eriti panga- ja krediitkaarditeenuse kaudu);
3. oht sõnumisaladuse rikkumisele (eriti sideteenuse puhul);
4. inimese asukoha reaalajas jälitamine (eriti sideteenuse puhul);
5. inimese majandusliku seisuga avalikuks saamine (eriti maksuandmete, pangaandmete ning krediidireitingu andmete kaudu – kuid ei hõlma avalike andmete kasutamist);
6. oht õiguslike tagajärgedega või samalaadse mõjuga diskrimineerimiseks (sealhulgas töövahendusteenuses ning palga- ja karjäärivõimalusi mõjutavas hindamisteenuses);
7. laste isikuandmete töötlemine (lastele suunatud teenustes);
8. seadusest tuleneva saladuse hoidmise kohustusega kaitstud teabe avalikuks saamise oht (juurdepääsupiiranguga teave, ameti- ja kutsesaladusega kaitstud teave).

Juhime tähelepanu, et slaidil kirjeldatud kriteeriumid ei kehti piiriülese andmetöötuse puhul.

## TAGAJÄRJED ANDMESUBJEKTILE

- õiguslike tagajärgedega otsus
  - mõjutab otseselt andmesubjekti juriidilisi õigusi
- muu märkimisvärne mõju
  - mõjutab märkimisväärselt isiku olukorda, käitumist või valikuid
  - avaldab pikaajalist või püsivat mõju
  - võib tuua kaasa tõrjutuse või diskrimineerimise

Profiilialalüüsi otsustega seotud suur oht on, et keegi jääb teiste tegude tõttu oma võimalustest ilma. Andmesubjektile tekkivate tagajärgede puhul eristatakse selgelt õiguslike tagajärgedega otsuseid (näiteks õigus saada konkreetset õigusaktidega kehtestatud sotsiaalhüvitist või selle hüvitise andmisest keeldumine; riiki sisenemise keelamine või kodakondsuse andmisest keeldumine jne) ning muud märkimisväärselt mõju (näiteks otsused, mis mõjutavad kellegi juurdepääsu terviseteenustele; otsused, millega võetakse ära kellegi töövõimalus või pannakse ta väga ebasoodsasse olukorda; otsused, mis mõjutavad kellegi juurdepääsu haridusele, näiteks ülikooli vastuvõtmist).

## MÕJUHINNANGU ELEMENDID

- kavandatud toimingud, eesmärgid
- vajalikkuse ja proportsionaalsuse analüüs
- ohtude kirjeldus ja hinnang
- kaitsemeetmed

Iga mõjuhinna kohustuslikud elemendid on lühidalt kirjeldatud IKÜM artikli 35 lõikes 7. Järgnevalt vaatleme ühte võimalikku sisulist lähenemist neile elementidele. Kindlasti oleneb mõjuhinna täpne ülesehitus konkreetse planeeritava toiminguga eripäradest.

## MÕJUHINNANGU LÄBIVIIMINE

- kirjelda plaanitud töötlemistoimingut (sh tehniline lahendus)
  - kaardista esialgselt võimalikud riskid (oht, tõenäosus, tagajärg)
  - moodustada tööühm
  - hinnata: vajalikkust, proportsionaalsust, riske
  - riskide maandamine
  - hinnata: vajalikkust, proportsionaalsust, riske
- ... (jätkub)



Iga töötlemistoimingu planeerimisel tuleb esimese sammuna detailselt kirjeldada planeeritud töötlemistoimingut. Andmeanalüütika kontekstis peaks selline kirjeldus kindlasti sisaldama ka kasutatava tehnilise lahenduse kirjeldust. Seejärel tuleks kaardistada esialgsed võimalikud riskid, et teha järeldus võimaliku suure ohu esinemise kohta. Kui suur oht on ilmne või selleks on vähemalt kahtlus, tuleks otsustada mõjuhinna läbi viimise kasuks.

Mõjuhinna läbiviimiseks tasub moodustada tööühm, kuhu on kaasatud olulisemad valdkondade esindajad, sh andmekaitseametnik, IT-spetsialist, andmeanalüütik ja võimalusel ka andmesubjektid või nende esindaja.

Mõjuhinna fookus peaks olema võimalikul tekkival kahjul, pidades silmas nii varalist kui ka mittevaralist kahju. Mõjuhinna eesmärk ei ole kõiki riske välistada, vaid riskid tuvastada ning need võimalusel maandada. Seejärel tuleb hinnata jääkriski - kas jääkrisk on põhjendatud. Vajadusel tuleb riskide hindamist, maandamist ja uuesti hindamist läbi viia korduvalt.

Käsitlesime koolituse käigus ka praktikas tõusetunud mõjuhinna vajadust andmetöötlustoimingut (näiteks sõidukite asukoha jälgimise puhul).

## MÕJUHINNANGU LÄBIVIIMINE

... (jätk)

- kui riskid on piisavalt maandatud, jätkata toimingute planeerimist
- kui riskid ei ole maandatud ja jääb suur risk, kaaluda järelvalveasutusega eelkonsulterimist
  
- DOKUMENTEERI
- vajadusel uuenda

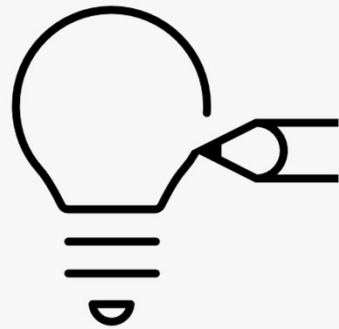
Mõjuhindangu lõppfaasis peaks selguma, kas võimaliku suure ohu riski on suudetud rakendatud meetmetega piisavalt maandada või mitte. Kui riskid on maandatud, võib edasi liikuda toimingute planeerimise ja selle läbi viimisega. Kui riskid ei ole maandatud ja mõjuhindangust nähtub, et isikuandmete töötlemise tulemusena tekiks jätkuvalt suur oht, peab vastutav töötleja enne isikuandmete töötlemist konsulteerima järelvalveasutusega või loobuma oma senisest plaanist.

Rõhutame, et mõjuhindangu läbi viimise iga sammu tasub detailselt dokumenteerida. Mõjuhindangu koostamise lõpus tuleb kindlasti koostada ka üks protsessi kokku võttev dokument, kuid dokumenteerimise protsessi tuleb juurutada juba mõjuhindangu läbi viimise käigus. Nagu juba eespool märgitud ei ole mõjuhindang ühekordselt läbi viidav toiming, vaid seda tuleb vajadusel täiendada ja uuendada. Seda nii toimingute muutumise puhul kui kindlasti ka siis, kui töötlemise käigus ilmneb asjaolusid, mida esialgses mõjuhindangus piisavalt ei arvestatud.



## MÕJUHINNANG – SAMM 1 – KIRJELDUS

- ajaline raamistik
- töötlemise laad
- töötlemise ulatus
- kasutatavad tehnilised lahendused
- kontekst, sh hinnang lähteandmestikule
- eesmärgid
- vajadus, proportsionaalsus



Üks võimalik lähenemine töötlemistoimingu kirjelduse etappidele mõjuhinnangus.

## MÕJUHINNANG – SAMM 2 – RISKID

- ohud (st mis võib juhtuda?)
- riskiga seotud isikuandmete kategooria
- tekkiva kahju tõenäosus
- mõju andmesubjektile
- KAS SUUR RISK?



Üks võimalik lähenemine riskide kirjelduse etappidele mõjuhinnangus.

## NÄIDE

Severity of impact	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		



## MÕJUHINNANG – SAMM 3 – RISKIDE MAANDAMINE

- meetmed riski maandamiseks
- meetme mõju riskile (välistab riski, maandab riski, kaalutud risk)
- tulemus, jääkrisk
- KAS SUUR RISK?

Üks võimalik lähenemine riskide maandamise kirjelduse etappidele mõjuhinnangus.

Riskide maandamise meetmeteks võib olla näiteks otsus, et teatud tüüpi andmeid siiski ei koguta või vähendatakse töötlemise ulatust. Samuti võib andmeanalüütika mudelite väljatöötamise puhul adekvaatseks meetmeks olla töödeldavate isikuandmete säilitamisperioodide minimaliseerimine, täiendavate tehnoloogiliste turvameetmete kasutusele võtmine või võimaluse korral isegi andmete anonüümimine või vähemalt pseudonüümimine.

Riskide maandamiseks sobivad kindlasti ka korralduslikud meetmed nagu personali koolitamine riskide ennetamise ja maandamise tagamiseks, riskide vältimiseks sisemiste juhiste ja eeskirjade koostamine ning koostööpartneritega rangemate lepingutingimuste kokku leppimine.



## Lõimitud andmekaitse (privacy by design)

Töötlemisvahendite  
kindlaksmääramisel ja töötlemise  
ajal

rakendatakse tehnilisi ja  
korralduslikke meetmeid,

mis aitavad kaasa määruse  
nõuete täitmisele

(sh andmesubjekti õiguste  
kaitsmisele).



Võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning töötlemise laadi, ulatust, konteksti ja eesmärgi, samuti töötlemisest tulenevaid füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte, rakendab vastutav töötleja nii töötlemisvahendite kindlaksmääramisel kui ka isikuandmete töötlemise ajal asjakohaseid tehnilisi ja korralduslikke meetmeid, nagu pseudonümiseerimine, mis on vajalikud andmekaitsepõhimõtete (nagu võimalikult vähete andmete kogumine) tõhusaks rakendamiseks ja vajalike kaitsemeetmete lõimimiseks isikuandmete töötlemisse, et täita käesoleva määruse nõudeid ja kaitsta andmesubjektide õigusi.

Lühidalt võib laadi mõista kui töötlemisele omaseid tunnuseid. Ulatus viitab töötlemise mahule ja piiridele. Kontekst on seotud töötlemise asjaoludega, mis võivad mõjutada andmesubjekti ootusi, ning eesmärk hõlmab töötlemise eesmärgi.

## Vaikimisi andmekaitse (*privacy by default*)

Vaikimisi töödeldakse ainult andmeid, mis on vajalikud konkreetse eesmärgi saavutamiseks.



Vastutav töötleja rakendab asjakohaseid tehnilisi ja korralduslikke meetmeid, millega tagatakse, et vaikimisi töödeldakse ainult isikuandmeid, mis on vajalikud töötlemise konkreetse eesmärgi saavutamiseks.

See kehtib kogutud isikuandmete hulga, nende töötlemise ulatuse, nende säilitamise aja ja nende kättesaadavuse suhtes. Nende meetmetega tagatakse eelkõige see, et isikuandmeid ei tehta vaikimisi ilma asjaomase isiku sekkumiseta määramata füüsiliste isikute ringile kättesaadavaks. Mõiste „vaikimisi“ viitab eelnevalt olemasolevale või eelvalitud seadistuse väärtusele, mis on määratud tarkvararakendusele, arvutiprogrammile või seadmele.



Sageli tekitab küsimusi, kas isikuandmete töötlemisel tohib kasutada pilveteenuseid. Sellele ei ole ühest jah/ei vastust. Isikuandmete pilves töötlemisele tuleb läheneda volitatud töötleja kaasamisele kehtestatud õigusliku raamistiku kaudu. Vastutav töötleja võib osa töötlemistoimingutest anda konkreetse ülesandena teisele isikule ehk volitatud töötlejale. Seejuures peab aga vastutav töötleja jätkuvalt tagama, et isikuandmed on piisavalt kaitstud ja töötlemine toimub vastavalt IKÜM nõuetele.



## VOLITATUD TÖÖTLEJA KAASAMINE

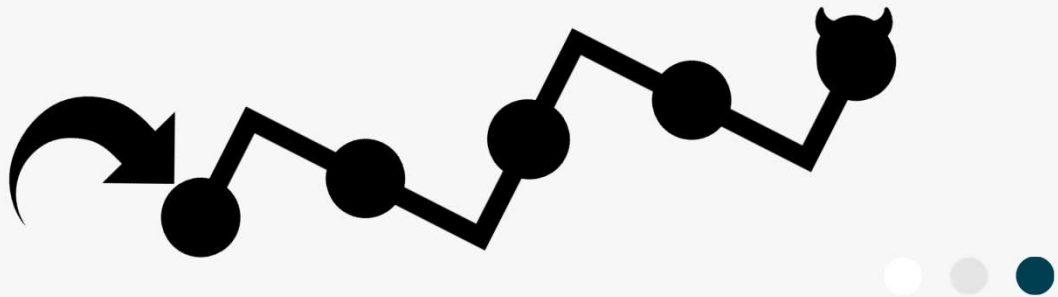
- vastutav töötleja ainult selliseid volitatud töötlejaid, kes
  - **annavad piisava tagatise** (providing sufficient guarantees), et
  - **nad rakendavad asjakohaseid tehnilisi ja korralduslikke meetmeid** sellisel viisil, et
  - **töötlemine vastab käesoleva määruse nõuetele ja sealjuures tagatakse andmesubjekti õiguste kaitse.**
- **Kuidas kontrollida piisavat “tagatist”?**

Volitatud töötleja kaasamisel (sh pilveteenuse jaoks) peab läbi mõtlema, kas vastutavalt töötlejal on võimalik volitatud töötleja tegevust piisavalt kontrollida. Vastutaval töötlejal peab alati säilima kontroll kõikide tema vastutusallas olevate isikuandmete üle.

Piisava tagatise kontrollimiseks on praktikas leitud erinevaid lahendusi. Põhjalikumad kontrollijad saavad detailseid küsimustike või palutakse edastada isikuandmete kaitset käsitlevad sisekorrad. Pahatihti piirduakse aga vastupidise äärmusega ehk küsitakse ainult mõni üksik küsimus ning rahuldutakse mõnesõnaliste vastusega. Ilmselt on kõige parem lahendus jällegi tasakaalus ehk kahe äärmuse keskel. Volitatud töötleja üle teostatav kontroll peaks olema piisavalt põhjalik, et veenduda koostööpartneri usaldusväärsuses, kuid liiga detailne sekkumine koostööpartneri siseasjadesse ei ole põhjendatav ka IKÜM nõuete täitmisega.

## VOLITATUD TÖÖTLEJA KAASAMINE

- **Volitatud töötleja** ei kaasa **teist volitatud töötlejat** ilma vastutava töötleja **eelneva** konkreetse või üldise **kirjaliku loata**
- Üldise kirjaliku loa korral teavitamiskohustus



Vastutavalt töötlejal peab alati säilima kontroll või vähemalt ülevaade volitatud töötleja kaasatud all-töötlejate kohta. IKÜM mõte on vältida olukorda, kus vastutav töötleja (ja seeläbi ka andmesubjekt) kaotab kontrolli andmete üle.

Praktikas tõusetub sellega sageli probleeme, sest ettevõtted ei taha ärisaladuste tõttu anda täit ülevaadet oma koostööpartneritest. Ettevõtted muretsevad sageli, et oma koostöövõrgustikust täieliku ülevaate andmisel lõigatakse nemad „vahendajana“ ära ja aetakse asja otse all-töötlejatega. Kuigi vahel on selline risk olemas, siis sageli püütakse „ärisaladuse“ kaitse taha pügeda siiski lihtsalt mugavusest. Isikuandmete kaitse nõuab maksimaalset läbipaistvust, kuid see peab olema tasakaalus muude põhiõigustega, sh ärisaladuse kaitsega.

## VOLITATUD TÖÖTLEJA KAASAMINE

- *Data Processing Agreement (DPA)*
- Vastutava töötleva ja volitatud töötleva vaheline leping
- Peab määrama:
  - töötlemise sisu ja kestus
  - töötlemise laad ja eesmärk
  - isikuandmete liik ja andmesubjektide kategooriad
  - vastutava töötleva kohustused ja õigused
- Kui ettenähtud eesmärki/vahendeid ületatakse, siis võib muutuda iseseisvaks vastutavaks töötlevaks (st lisandub kohustusi)

Volitatud töötleva kohustused vastutava töötleva ees tuleb määrata kindlaks lepinguga või õigusakti alusel. Vastutustundlik andmetöötlus tähendab ühtlasi, et vastutav töötleva on sõlminud koostööpartneritega õiguspärased andmetöötluslepingud.

Andmetöötluslepingus on sätestatud nõuded, mida vastutav töötleva ja volitatud töötleva peavad andmete töötlemisel järgima. See hõlmab andmete säilitamise, kaitsmise, töötlemise, juurdepääsu ja kasutamise tingimuste seadmist. Lepingus on ka määratletud, mida volitatud töötleva võib andmetega teha ja mida mitte. Tegemist on mõlema poole huve kaitsva dokumendiga, mis lisaks isikuandmete kaitsesele tagab ka poolte enda huvide parema kaitse järelevalvemenetluses.

W A L L E S S

W A L L E S S

AITÄH!

Liivalaia 45, 10145 Tallinn  
Kaluri 2, 51004 Tartu

[www.walless.com](http://www.walless.com)

