Õigus olla unustatud või kohustus olla mäletatud?

Isikuandmete kaitsest mäluasutustes

13.03.2018

Tiina Ilus

Building a better working world

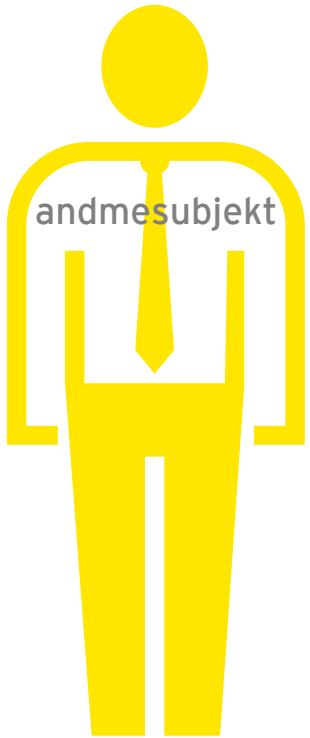
1. Andmekaitse õiguslik raamistik

- Kaasaegse andmekaitse põhireeglid on samad juba peaaegu nelikümmend aastat.
- Euroopa Liidu andmekaitse õiguslik raamistik on sama juba üle kahekümne aasta.
- EL-i andmekaitse reform – uus algus?
- Määrus füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (*General Data Protection Regulation* ehk **GDPR**) jõustub 25.05.2018.
- Eesmärgid:
  - üksikisiku autonoomiat austavad kõrged andmekaitsestandardid, ent ka piirideta toimiv andmemajandus (andmed kui „uus nafta“?)
  - JÕUSTATAVUS!

2. Isikuandmed ja töötlemise aluspõhimõtted

Isikuandmed

- „igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta“
- Tuvastav tunnus ei pea olema nimi (Jaan Tamm vs kikilipsuga nätsunärija)
- Eriliiki isikuandmed (delikaatsed isikuandmed)



Põhimõtted

- seaduslikkus, õiglus ja läbipaistvus
- eesmärgi piirang
- võimalikult väheste andmete kogumine
- andmete õigsus
- säilitamise piirang
- usaldusväärsus ja konfidentsiaalsus
- vastutus (*accountability*)

3. Millal tohib isikuandmeid töödelda?

- Andmesubjekt on andnud oma nõusoleku
- Andmesubjektiga sõlmitud lepingu täitmiseks
- Juriidilise kohustuse täitmiseks
- Andmesubjekti või muu füüsilise isiku eluliste huvide kaitseks
- Avalikes huvides oleva ülesande täitmiseks või avaliku võimu teostamiseks
- Õigustatud huvi korral, v.a kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, eriti juhul, kui andmesubjekt on laps – EI KOHALDU AVALIKU SEKTORI ASUTUSTELE

Erand: avalikes huvides toimuv andmete kasutamine arhiveerimise, teadus- ja ajaloouuringute või statistilisel eesmärgil

4. Nõusolek isikuandmete töötlemiseks

- „vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega“, eriliigiliste andmete puhul lisaks ka „selgesõnaline“.
- Nõusoleku küsimise tingimused:
  - arusaadaval ja lihtsasti kättesaadaval kujul,
  - kasutades selget ja lihtsat keelt.
- Nõusolekut peab töötleja igal hetkel saama tõendada.
- Andmesubjekt peab saama nõusoleku igal hetkel tagasi võtta. Sellest tuleb eelnevalt teavitada ja tagasivõtmine peab olema vähemalt sama lihtne, kui oli selle andmine.
- Nõusolek isikuandmete töötlemiseks peab olema eristatud muudest tingimustest.

5. Kohustused andmesubjekti ees (1/2)

1. **Andmesubjekti teavitamine andmete kogumisel**
2. **Andmesubjekti juurdepääsuõigus oma andmetele**
3. **Valede andmete parandamine**
4. **Õigus olla unustatud ja töötlemise lõpetamine**
5. ***Andmete väljastamine ja ülekandmine***
6. ***Õigus mitte lubada automatiseeritud otsuseid***

5. Kohustused andmesubjekti ees (2/2)

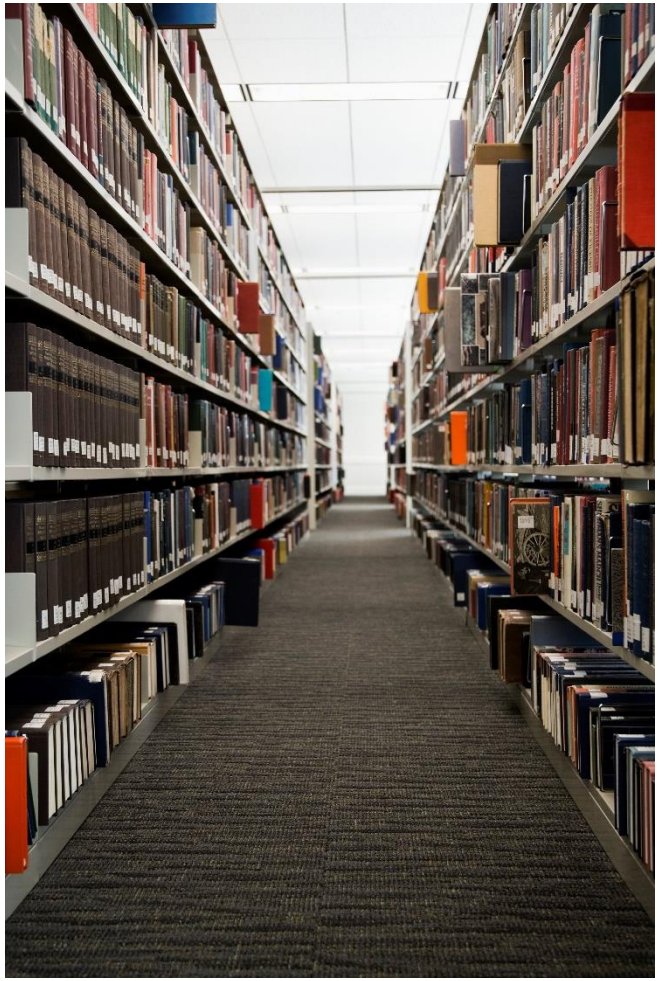
- Isikuandmete töötlemine peab olema andmesubjekti jaoks võimalikult läbipaistev.
- Andmesubjektidele tuleb teatavaks teha:
  - kes on vastutav töötleja, esindaja ja andmekaitseametniku kontaktandmed;
  - milline on töötlemise õiguslik alus (huvide kaalumise korral põhjendus);
  - kellele andmeid võidakse väljastada;
  - andmete säilitamise tähtaeg (või selle määramise kriteeriumid);
  - tema õigused (juurdepääs, vastuväited, parandamine);
  - õigus nõusolek tagasi võtta;
  - kas isikuandmete esitamine on õigusaktist või lepingust tulenev kohustus või lepingu sõlmimiseks vajalik nõue;
  - teave automatiseeritud otsuste, sealhulgas profiilianalüüsi tegemise kohta.

24. veebruaril kell 13.00 kutsub Eesti Pressifotograafide Liit kõiki Eesti elanikke ja külalisi jäädvustama ajaloolist hetke ning pildistama ühe minuti jooksul ümbritsevaid inimesi, meeleolusid, objekte või loodust. Kõik aktsiooni käigus tehtud pildid kogutakse kokku ja edastatakse koos autori nime ja kujutatu kirjeldusega säilitamiseks Eesti Rahva Muuseumi. Piltidest sünnib Eesti ajaloo suurim fotonäitus, need avaldatakse meie veebikeskkonnas ja osaliselt ka meedias.

- Kes on vastutav töötleja? Riigikantselei? Eesti Pressifotograafide Liit? ERM?
- Milline on õiguslik alus? Avalik ülesanne? Nõusolek (ja sel juhul kelle)? Pildi saatis fotograaf, kes ilmselt enamikel juhtudel ise pildil ei ole.
- Olemas on eesmärgi ja lubatava üleandmise (ERM) ja avalikustamise (Eesti suurim fotonäitus) tingimused.
- Mida peab tegema suitsetav trammijuht, kui ta leiab end eestiminut.ee avalehelt?

6. Arhiveerimine, teadustöö ja statistika

- Isikuandmete (s.h eriliigiliste andmete) töötlemine avalikes huvides toimuva arhiveerimise, teadus- ja ajaloouuringute või statistilisel eesmärgil on lubatud: see ei riku eesmärgi piirangu nõuet ega säilitamise piirangu nõuet.
- Nõutavad on kaitsemeetmed andmesubjekti õiguste ja vabaduste kaitseks, eelkõige selleks, et tagada võimalikult väheste andmete kogumise põhimõtte järgimine, s.h pseudonümiseerimine.
- Lubatud on siseriikliku õigusega piirata isiku õigusi andmetele juurdepääsuks ja andmetöötlusele vastuväidete esitamiseks.



7. Teadusuuringuks isikuandmete töötlemine

Isiku nõusolek	▶ „vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega“, eriliigiliste andmete puhul lisaks ka „selgesõnaline“
Anonüümsed andmed	▶ Kui tegemist ei ole (enam) isikuandmetega, IKS ega GDPR ei kohaldu
AKI loal ja eritingimustel	▶ AKI luba isikustatud andmete kasutamiseks, kui on täidetud teatud nõuded.

8. Teadustöö ja statistika – IKS eelnõu (1/2)

- Isikuandmete töötlemine andmesubjekti nõusolekuta on lubatud teadusuuringu või riikliku (!) statistika vajadusteks eelkõige pseudonümiseeritud kujul. Enne isikuandmete üleandmist asendatakse isiku tuvastamist võimaldavad andmed isikut mittetuvastavate andmetega. Depseudonüümimine on lubatud ainult täiendavate teadusuuringute või riikliku statistika vajadusteks.
- Isikustatud kujul töötlemine on lubatud ainult juhul, kui:
  - isikustamata kujul ei ole võimalik eesmärki saavutada;
  - kui selleks on teadusuuringu teostaja hinnangul ülekaalukas avalik huvi;
  - see ei pane andmesubjektile lisakohustusi ega kahjusta tema õigusi ülemääraselt;
  - kasutatakse kaitsemeetmeid (vt järgmine slaid).
- AKI **eelkontroll**, kuulates vastavas valdkonnas seaduse alusel loodud eetikakomitee olemasolu korral ära ka selle seisukoha.

8. Teadustöö ja statistika – IKS eelnõu (2/2)

- Eriliiki andmete töötlemine on lubatud üksnes seaduse alusel, avalikes huvides toimuva teadusuuringu või statistilisel eesmärgil ning töötlemine on proportsionaalne saavutatava eesmärgiga ning tagatud on järgmiste asjakohaste meetmete kasutamine:
  - tehnilised ja korralduslikud kaitsemeetmed;
  - andmetöötlustoimingute logimine;
  - andmekaitseametnik;
  - pseudonümiseerimine;
  - krüpteerimine.
- Lubatud on piirata andmesubjekti juurdepääsuõigust, andmete parandamise õigust ning õigust esitada vastuväiteid, kui vastasel juhul muutuks võimatuks eesmärgi saavutamine või see oleks oluliselt takistatud.

9. Avalikes huvides arhiveerimine – IKS eelnõu

- Andmete töötlejal on lubatud piirata isiku õigusi:
  - andmetele juurdepääsuks niivõrd, kuivõrd arhiivimaterjali ei ole inimese nime kaudu identifitseeritud või kui materjali ei ole mõistliku pingutusega võimalik üles leida;
  - nõuda andmete parandamist;
  - nõuda andmete väljastamist ja ülekandmist (kohalduks nagunii vaid juhul, kui töötlemise õiguslik alus on nõusolek või lepingu täitmine);
  - esitada andmete töötlemisele vastuväiteid.

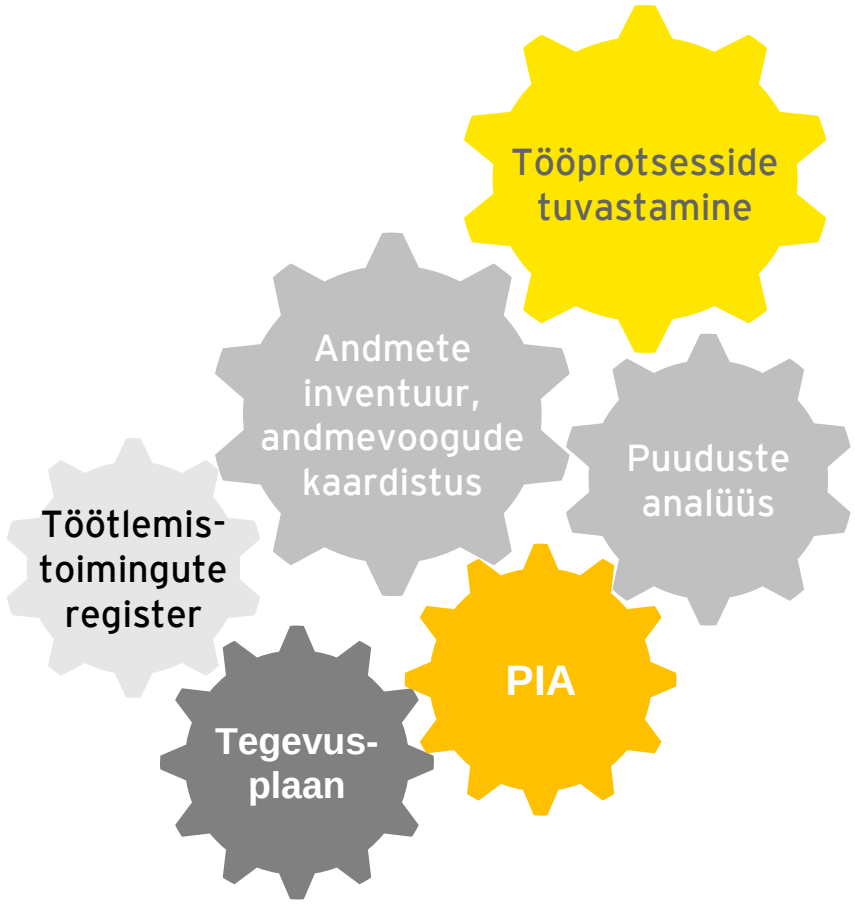
10. Andmekaitsespetsialist (*data protection officer* ehk DPO)

- Osa isikuandmete töötleja sisulisemast vastutusest (*accountability*).
- Laia profiiliga andmekaitse eestkõneleja!
- Kohustuslik nii vastutavale kui volitatud töötlejale, kui:
  - isikuandmeid töötleb avaliku sektori asutus või organ (avaliku ülesande täitja)
  - põhitegevuse moodustavad isikuandmete töötlemise toimingud, mille laad, ulatus ja/või eesmärk tingivad ulatusliku andmesubjektide korrapärase ja süstemaatilise jälgimise
  - põhitegevuse moodustab andmete eriliikide ja süütegudega seotud isikuandmete ulatuslik töötlemine.
- Avaliku sektori asutus või organ võib määrata ühe andmekaitseametniku olenevalt nende organisatsioonilisest struktuurist ja suurusest.
- Koosseisuline töötaja või teenuslepingu alusel (väline DPO).
- JuM koostatud GDPR mõjuhinnangu kohaselt on ainuüksi avalikus sektoris 2829 asutust, kellel on DPO määramine kohustuslik.

11. Veel GDPR-i uuendusi

1. Isikuandmetega seotud rikkumisest teavitamine
2. Riskide ja andmekaitsemõjude pidev hindamine
3. Lõimitud ja vaikimisi andmekaitse
4. Volitatud töötleja iseseisev vastutus
5. Andmetöötlus-toimingute register
6. EL-i piire ületav mõju ja trahvid

12. Olulised sammud GDPR-iks valmistumisel



- Isikuandmetega seotud tööprotsesside tuvastamine
  - põhiprotsessid
  - tugiprotsessid
- Andmete ja andmevoogude kaardistamine
  - isikute gruppide ja andmete tuvastamine
  - andmete töötlemise aluse määratlemine
  - andmevoogude (sh siseste, väliste) kaardistamine
- Puuduste analüüs (*gap analysis)*
  - küsimustike põhjal olukorra hindamine ja puuduste tuvastamine
- Privaatsuse mõjuhinnang (*DPIA*)
  - tehakse andmetöötlusprotsesside kohta (valikuliselt)
  - hinnatakse mõju isiku privaatsusele
- Isikuandmete töötlemise toimingute registreerimine (*ROPA*)
- Tegevusplaani koostamine

13. Turundusinfo saatmine

- Otseturundus hõlmab mistahes teadaandeid, mis otseselt või kaudselt edendavad selle saatja huve: pakkumised, kampaaniad, uudiskirjad jms.
- Tehnoloogianeutraalne: ükskõik, millist elektroonilist kommunikatsioonikanalit kasutatakse (e-mail, sms, mms, suhtlusplatvorm vms).
- Otseturundus on lubatud vaid isiku nõusolekul, mis peab vastama GDPR-i tingimustele (*opt-in*).
- Nõusolekut peab saama igal hetkel tagasi võtta ja seda õigust tuleb regulaarselt meelde tuletada.
- Erandina on lubatud ilma nõusolekuta turundusteadaandeid saata olemasoleva kliendisuhte raames sarnaste toodete või teenuste pakkumiseks ja kliendil peab olema võimalus iga hetk selliste teadete saatmine keelata (*opt-out*).

Aitäh kuulamast!