MILLELE PEAB KOOL ANDMEKAITSE ISIKUANDMEKAITSE ÜLDMÄÄRUSE OSAS TÄHELEPANU PÖÖRAMA?

Hanno Saks (DPO)

KAKS LÄHENEMIST

Opt-in: Isikuandmete ja privaatsuse kaitse on põhiõigus (EL)

Opt-out: Keelatud on kahjutegeval viisil kasutamine (näiteks: USA)

ANDMETE ELUTSÜKKEL

Loomine

Säilitamine

Kasutamine

Arhiveerimine

Hävitamine

MÕISTED

Vastutav töötleja

Volitatud töötleja

Kaasvastutav töötleja

MÕISTED

Pseudonüümiseerimine

Isikuandmetega seotud rikkumine – turvanõuete rikkumine, mis põhjustab andmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu.

Terviseandmed

ERAELU

Põhiseadus §19. Igaühel on õigus vabale eneseteostusele.

Igaüks peab oma õiguste ja vabaduste kasutamisel ning kohustuste täitmisel austama ja arvestama teiste inimeste õigusi ja vabadusi

Põhiseadus §26. Igaühel on õigus perekonna- ja eraelu kaitsele.

Põhiseadus §43. Igaühel on õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele.

Piirid ja sisu otsustab igaüks ise.

LASTEKAITSE

ÜRO Laste õiguste konventsioon
Artikkel 16
1. Mitte ühegi lapse eraellu, perekonnaellu, kodusse ega kirjavahetusse ei või meelevaldselt ega ebaseaduslikult sekkuda, samuti ei tohi ebaseaduslikult rünnata tema au ja head mainet.
2. Lapsel on õigus seaduslikule kaitsele niisuguse vahelesegamise ja rünnakute vastu.

PGS
§ 29. Õpilase hindamine
§ 35. Õppes osalemine ja koolis korraldatavast õppest puudumine
§ 37. Õpilase arengu toetamine
§ 46. Haridusliku erivajadusega õpilane

Lastekaitse seadus
§ 11. Lapse sotsiaalsed õigused
§ 13. Lapse õigus privaatsusele

GDPR KEHTIVUS

Ei kohaldata:

1. töödeldakse tegevuse käigus, mis ei kuulu EL õiguse kohaldamisalasse;
2. riigiasutus töötleb välis- või julgeoleku poliitika elluviimiseks;
3. **füüsiline isik töötleb eranditult isiklike või koduste tegevuste käigus**
4. töötlejaks on õiguskaitseorgan

ISIKUANDMETE TÖÖTLEMISE SEADUSLIKKUS

Töötlemine on seaduslik kui:

- andmesubjekt on andnud nõusoleku

- lepingulised suhted;

- vajalik töötleja juriidilise kohustuse täitmiseks;

- füüsilise isiku eluliste huvide kaitsmiseks;

- seadustest tulenev õiguspärane tegevus;

- õigustatud huvi; (v.a. andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb kaitsta isikuandmeid, eriti juhul kui andmesubjekt on laps).

TÖÖTLEMISE PÕHIMÕTTED

Isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus.

Isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt.

Isikuandmed peavad olema õiged ja vajaduse korral ajakohastatud ning et võetakse kõik mõistlikud meetmed, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutaks või parandataks viivitamata.

Isikuandmeid võib säilitada kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse.

Isikuandmeid võib töödelda viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid.

INFOÜHISKONNA TEENUS

Infoühiskonna teenuse pakkumisel otse lapsele on tema isikuandmete töötlemine seaduslik ainult juhul kui ta on 16 aastane või vanem.

Noorema puhul ainult juhul, kui on olemas eestkostja nõusolek.

Ei mõjuta liikmesriikide üldist lepinguõigust. Sic!

NÕUSOLEK

Nõusoleku olemasolu peab tõendama töötleja.

Kirjaliku nõusoleku taotlus peab arusaadavalt ja lihtsasti kättesaadaval kujul, selges ning lihtsas keeles olema selgelt eristatav muust dokumendist.

Nõusoleku võib igal ajal tagasi võtta.

Tagasivõtmine ei oma tagasiulatuvat jõudu.

Nõusoleku tagasivõtmise õigusest tuleb teavitada enne nõusoleku andmist.

NÕUSOLEK

Ei ole vajalik:

- lepingu täitmine või lepingu täitmise tagamine;
- töötleja kohustuste täitmine;
- isiku eluliste huvide kaitsmiseks;
- avalikes huvides või avaliku võimu teostamisel,
- õigustatud huvi korral.

ISIKUANDMED

Isikuandmed – igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta.

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

Kõik tegevused on töötlemine (isegi postkasti vaatamine kus *VÕIVAD* olla isikuandmetega info)

ERILIIGILISED ISIKUANDMED

Andmed millest ilmnevad:

- rassiline või etniline päritolu;
- poliitilised vaated;
- usulised või filosoofilised veendumused;
- ametühingusse kuulumine;
- geneetilised andmed;
- biomeetrilised andmed;
- terviseandmed;
- andmed isiku seksuaalelu või seksuaalse sättumuse kohta.

LÄBIPAISTVUS

Läbipaistvus – isikule esitatav teave tema andmete töötlemisest peab olema kokkuvõtlik, arusaadav, lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt.

Kui andmed on kogutud andmesubjektilt, siis tuleb talle isikuandmete saamise ajal teatavaks teha:

- vastutava töötleja ja töötleja esindaja nimi ja kontaktandmed;

- andmekaitseametniku kontaktandmed;

- isikuandmete töötlemise eesmärk ja õiguslik alus;

- kui isikuandmete töötlemine põhineb töötleja või kolmanda isiku õigustatud huvil, siis info, millisel alusel põhineb õigustatud huvi;

- teave isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta;

ÕIGUSTATUD HUVI

Õigustatud huvi võib olla töötlemise aluseks, kui isiku huvid või põhiõigused- ja vabadused ei ole tähtsamad.

Õigustatud huvi võib olla siis, kui isik on töötleja klient või töötab tema juures.

Õigustatud huvi on ka isikuandmete töötlemine tagamaks võrgu- ja andmeturve.

Õigustatud huvi on ka isikuandmete edastamine seoses võimalike süütegudega ja avalikku julgeolekut ähvardavate ohtudega.

Jälgida tuleb, et see oleks kooskõlas õigusliku, kutsealase või muu saladuse hoidmise kohustusega.

Töötleja peab tõendama, et tema õigustatud huvid kaaluvad üles isiku huvid või põhiõigused ja vabadused.

RIKKUMISEST TEAVITAMINE

Teates tuleb:

- kirjeldada rikkumise laadi ning nimetada andmesubjektide kategooriad ja ligikaudne arv ning isikuandmete kirjete liigid ja ligikaudne arv;

- teatada andmekaitsespetsialisti või kontaktisiku nimi ja kontaktandmed;

- kirjeldada rikkumise võimalikke tagajärgi;

- kirjeldada võetud või võtmiseks kavandatud meetmeid rikkumise lahendamiseks, sealhulgas vajaduse korral rikkumise võimaliku kahjuliku mõju leevendamiseks.

Isikut peab teavitama kui rikkumine kujutab endast tõenäoliselt suurt ohtu tema õigustele ja vabadustele.

Kõik rikkumised tuleb dokumenteerida.

ANDMETE KUSTUTAMINE

Õigus olla unustatud

1. Eesmärk on lõppenud
2. Tagasivõetud nõusolek
3. Töödeldakse ebaseaduslikult
4. Vastutava töötleja juriidilised kohustused
5. Koguti seoses infoühiskonnateenus pakkumisega
6. Peale kustutamist tuleb teavitada ka kaasvastutajaid ja seotud isikuid

POLE VAJA KUSTUTADA

- on ajakirjandus

- juriidiline alus kestab

- rahvatervise valdkonnas avaliku huviga seotud põhjustel;

- avalikes huvides toimuva arhiveerimise, teadus või ajaloouuringute või statistilisel eesmärgil;

- õigusnõuete koostamiseks, esitamiseks või kaitsmiseks.

TÖÖTLEMISE PIIRAMINE

- andmesubjekt vaidlustab isikuandmete õigsuse;

- isikuandmete töötlemine on ebaseaduslik, kuid andmesubjekt ei taotle isikuandmete kustutamist, vaid kasutamise piiramist;

- vastutav töötleja ei vaja isikuandmeid enam töötlemise eesmärkidel, kuid need on andmesubjektile vajalikud õigusnõuete koostamiseks, esitamiseks või kaitsmiseks,

- andmesubjekt on esitanud isikuandmete töötlemise suhtes vastuväite.

Piiramise korral võib isikuandmeid töödelda ainult:

- isiku nõusolekul;

- õigusnõuete koostamiseks, esitamiseks või kaitsmiseks;

- teiste isikute õiguste kaitsmiseks;

- olulise avaliku huvi korral.

INVENTUURID

Andmete inventuur

Eesmärkide inventuur

Kasutajate inventuur

Töötlemise kategooriate inventuur

Asukohtade inventuur

Riskide inventuur

Riskide maandamise inventuur

REGISTREERIMINE

Vastutav töötleja peab registreerima kõik isikuandmetega tehtavad toimingud.

Volitatud töötleja peab pidama töötlemise toimingute kategooriate registrit.

Registreerima ja registrit pidama ei pea siis, kui ettevõttes või organisatsioonis on vähem kui 250 töötajat. Välja arvatud:

- töötlemine kujutab tõenäoliselt ohtu isiku õigustele ja vabadustele;

- töödeldakse eriliiki isikuandmeid;

- töödeldakse kohtuotsuste ja süütegudega seotud andmeid;

- töötlemine ei ole juhtumipõhine.

DPO

Andmekaitsespetsialisti peab määrama:

- isikuandmeid töötlev avaliku sektori asutus või organ;

- töötleja kelle põhitegevuse moodustavad isikuandmete toimingud, mis hõlmavad ulatuslikku isikute korrapärast ja süstemaatilist jälgimist;

- töötleja kelle põhitegevuse moodustavad andmete eriliikide ja süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete ulatuslik töötlemine.

Vastutav töötleja vastutab tekitatud kahju eest, kui töötlemisel on rikutud määrust.

Volitatud töötleja vastutab tekitatud kahju eest, kui on rikkunud konkreetselt temale suunatud määruse nõudeid või ta ei ole järginud vastutava töötleja antud juhiseid või tegutsenud nende vastaselt.

DPO

Nõuded andmekaitsespetsialistile:

- teadmine organisatsiooni väärtustest ja eesmärkidest;
- teadmine organisatsiooni toimimise protsessidest;
- teadmine töökorralduse reeglitest ja poliitikatest;
- teadmine üldistest isikuandmete kaitse õigusaktidest;
- teadmine organisatsiooni tegevusvaldkonna isikuandmete kaitse õigusaktidest;
- teadmine isikuandmete töötlemise mõjudest organisatsioonile ja andmesubjektile;
- teadmine IKT ja andmeturbe mõjudest andmesubjektile ja organisatsioonile;
- teadmine riskianalüüsist ja riskijuhtimisest;
- teadmine andmekaitsealasest mõjuhinnangust;

DPO AMETISEISUND

- peab olema tagatud nõuetekohane ja õigeaegne kaasamine kõikidesse isikuandmete kaitsega seotud küsimustesse;

- tuleb anda ülesannete täitmiseks ja ekspertteadmiste taseme hoidmiseks vajalikud vahendid ning juurdepääs isikuandmetele ja töötlemise toimingutele;

- ei saa juhiseid ülesannete täitmiseks;

- ülesannete täitmise eest ei tohi ametist vabastada ega karistada;

- allub otse töötleja kõrgeimale juhtimistasandile;

- tema poole võib pöörduda kõigis küsimustes, mis on seotud andmesubjekti andmete töötlemise ja GDPR-ist tulenevate õiguste kasutamisega;

- seotud saladuse hoidmise ja konfidentsiaalsuse nõudega.

Võib täita muid ülesandeid ja kohustusi, kui need ei põhjusta huvide konflikti andmekaitsespetsialisti ülesannete ja kohustustega.

DPO ÜLESANDED

- teavitada ja nõustada töötlejat seoses andmekaitsenormidega;

- jälgida isikuandmete kaitse põhimõtete järgimist, sh vastutusvaldkondade jaotamist, personali teadlikkuse suurendamist ja koolitamist, seonduvat auditeerimist;

- nõustada seoses mõjuhinnanguga ja jälgida selle toimist;

- teha koostööd järelevalveasutusega;

- olla kontaktisik järelevalveasutuse jaoks.

Ülesannetest tulenevalt ei saa andmekaitsespetsialist olla see, kes isikuandmete töötlemisega seotud asjad ära teeb.

Ta kontrollib, et asjad oleks tehtud ja kooskõlas isikuandmete kaitse reeglitega.

MÕJUHINNANG

Isikuandmete töötlemisega kaasnevate ohtude ja riskide hindamine.

Teisisõnu kitsa suunitlusega (isikuandmete töötlemine) riskide hindamine (analüüs).

Isikuandmete töötlemine ei ole asi iseeneses.

Ainult abivahend organisatsioonile oma eesmärkide saavutamiseks ja seega lahutamatu osa töötleja tegevusstrateegiast.

IT on abivahend isikuandmete töötlemiseks.

Töötlemisel, eelkõige uute tehnoloogiate kasutamisel, kui tõenäoliselt või tekkida suur oht isikute õigustele ja vabadustele, peab enne töötlemist hindama kavandatavate toimingute mõju isikuandmete kaitsele.

Peab küsima ka andmekaitsespetsialisti arvamust.

MÕJUHINNANG

Mõjuhinnang on kohustuslik:

- automaatsel töötlemisel põhineval süstemaatilisel ja ulatuslikul hindamisel, mille alusel tehakse otsuseid, mis omavad õiguslikke tagajärgi või mõjutava oluliselt isikut;

- süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud andmete ulatuslikul töötlemisel;

- andmete eriliikide töötlemine;

- toimub avalike alade ulatuslik süstemaatiline jälgimine.

MÕJUHINNANG

Mõjuhinnangus peavad olema kirjeldatud:

- kavandatavad töötlemise toimingud;

- töötlemise eesmärkide süstemaatiline kirjeldus (sh õigustatud huvi);

- töötlemise toimingute vajalikkuse ja proportsionaalsuse hindamine eesmärkide suhtes;

- andmesubjektide õigusi ja vabadusi puudutavate ohtude hinnang;

- ohtude käsitlemiseks kavandatud meetmed isikuandmete kaitse tagamiseks ja määruse järgimise tõendamiseks.

MILLISED ON OHUD VÕI PUUDUSED KOOLIDES TEGEVUSE MÄÄRUSELE VASTAVUSSE VIIMISEL?

1. Tõlgendamine

1.1 Pidaja tasemel

1.2 Asutuse tasemel

2. Kompetents ja selle jagamine

3. Töötajate pidev teavitamine, harimine ja kontrollimine

4. Tehnoloogilised võimekused on äärmiselt ebaühtlased

5. Erinevate haridusasutuste erinev stardipakk

MILLISED ON HEAD NÄITED GDPR RAKENDAMISEL KOOLIS?

Headeks näideteks on see, et paljudes koolides on hakatud erinevate online app'ide kasutamisel tõsiselt mõtlema kasutajate/kasutamiste „anonümiseerimisele".

Selle üle pole seni väga palju mõeldud ja eesmärk on olnud alati, et kui midagigi tehtaks ja midagigi kasutataks, siis on JUBA väga hea. Nagu juba alguses sai öeldud, enamik GDPR'is kirjeldatust ja deklareeritust on kehtinud juba eelmisel kümnendil tänu toonaste ja ka praeguste valdkonnas tegevate professionaalide suurele tööle.

Nüüd on lisatud seni suhteliselt hambutule keskkonnale kihvad ja kontrollivad (kohustuslikult enesekontrollivad) silmad ning ehk saavad asjad ka paremaks, sest me kõik tahame, ükskõik kummal pool lauda ka istume, et meie kohta saadav/töödeldav info oleks meie soovidele vastav ning kontrollitav omaniku poolselt.

TÄNUD SUURED!!!

Hanno Saks (DPO)