Andmekaitse ja isikuandmete töötlemine

Anu Sander, vandeadvokaat
Kärt Raud, advokaat

Advokaadibüroo TGS Baltic
22.11.2017, Tartu

Ajakava

14:00 – 15:30	Koolitus
15:30 – 15:45	Paus
15:45 – 17:15	Koolitus

Mida peab teadma andmekaitsest ja isikuandmete töötlemisest?

Isikuandmete kaitse regulatsioon – olevik ja tulevik

Olevik:

- Isikuandmete kaitse seadus (IKS)
- Erinormid erinevates seadustes
- IKS põhineb andmekaitsedirektiivil 95/46/EÜ

Tulevik:

- Isikuandmete kaitse üldmäärus (ingl. k. *General Data Protection Regulation* – GDPR)
- Euroopa Parlamendi ja Nõukogu määrus - otsekohalduv kogu Euroopa Liidus alates 25. mai 2018
- Üldmääruse rakendamise seadus?
- Reformi põhjused

Isikuandmete kaitse - mida või keda me kaitseme?

- Eesmärk on kaitsta isikuandmete töötlemisel füüsilise isiku põhiõigusi ja -vabadusi, eelkõige õigust eraelu puutumatusele.
- Isikuandmete kaitse eesmärgiks ei ole kaitsta andmeid, vaid kaitsta inimest, keda kaitstavad andmed identifitseerivad ja mille kaudu isik ennast teistele isikutele määratleb.
- Õigus eraelu puutumatusele ja isikuandmete kaitsele kirjas muuhulgas:
  - Eesti Vabariigi põhiseaduses (PS)
  - Euroopa Liidu põhiõiguste harta
  - Euroopa Liidu toimimise leping
  - Inimõiguste ja põhivabaduste kaitse konventsioonis (EIÕK)

Millal isikuandmete kaitse üldmäärus kohaldub?

- Sisuline kohaldamisala: igasugusele isikuandmete töötlusele, va:
  - kui isikuandmeid töötleb füüsiline isik eranditult isiklike või koduste tegevuste käigus;
  - kui isikuandmeid töötlevad pädevad asutused süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise, sh avalikku julgeolekut ähvardavate ohtude kaitsmise ja ennetamise eesmärgil;
  - ühtse välis- ja julgeolekupoliitika valdkonnas;
  - EL õiguse kohaldamisalast väljaspool olevad valdkonnad
- Territoriaalne kohaldamisala:
  - kui töötleja tegevuskoht asub EL-is ning ta töötleb andmeid selle tegevuskoha kontekstis (sõltumata sellest, kus töötlemine ise toimub)
  - kui töötlemine on seotud EL-is asuvatele andmesubjektidele kaupade ja teenuste pakkumisega või nende tegevuse jälgimisega.

Mis on isikuandmed?

- Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta
- Neli elementi:
  - igasugune teave
  - tuvastatud või tuvastatav
  - füüsiline isik
  - kohta
- Tuvastatavuse kriteerium: 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 (GDPR Art 4 p 1; pp 26)

Isikuandmete liigitus

- Isikuandmed jagunevad:
  1) eriliigilised isikuandmed - GDPR Art 9 (IKS-is: delikaatsed isikuandmed)
  2) nn tavalised isikuandmed – mis tahes muud andmed inimese kohta, mis ei ole eriliigilised isikuandmed (nt nimi, sünniaeg, isikukood, näofoto, aadress, perekonnaseis, majanduslik seisund)
- Eriliigiliste isikuandmete kontseptsioon põhineb vajadusel anda teatud laadi andmetele suurem kaitse.

Eriliigilised isikuandmed (Art 9)

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

Isikuandmete töötlemine (Art 4 p 2)

Isikuandmete töötlemine on iga isikuandmetega tehtav toiming, sealhulgas:

- Kogumine
- Dokumenteerimine
- Korrastamine
- Struktureerimine
- Säilitamine
- Kohandamine
- Muutmine
- Päringute tegemine
- Lugemine
- Kasutamine
- Edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine,
- Ühitamine või ühendamine,
- Piiramine
- Kustutamine
- Hävitamine

Isikuandmete töötleja

- Vastutav töötleja (*controller*):
  - 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 (Art 4 p 7);
- Kaasvastutavad töötlejad (*joint controllers*)
  - määravad andmetöötluse eesmärgid ja vahendid ühiselt (Art 26). Jaotatakse omavahel kohustuste ulatus. Andmesubjekti ees vastutavad ühiselt (solidaarvastutus).
- Volitatud töötleja (*processor*):
  - füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel (Art 4 p 8);

Isikuandmete töötlemise põhimõtted (Art 5)

- Seaduslikkus, õiglus ja läbipaistvus (*lawfulness, fairness, transparency*)
- Eesmärgi piirang (*purpose limitation*)
- Võimalikult väheste andmete kogumine (*data minimisation*)
- Õigsus (*accuracy*)
- Säilitamise piirang (*storage limitation*)
- Usaldusväärsus ja konfidentsiaalsus (*integrity and confidentiality*)

Isikuandmete töötlemise õiguslikud alused (Art 6)

- Andmesubjekti nõusolek
- Vajalik andmesubjektiga sõlmitud lepingu täitmiseks
- Vajalik vastutava töötleja juriidilise kohustuse täitmiseks
- Vajalik andmesubjekti või muu füüsilise isiku eluliste huvide kaitsmiseks
- Vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks
- Vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral

Andmesubjekti nõusolek (Art 4 p 11, Art 7)

- Andmesubjekti nõusolek on tahteavaldus, mis on:
  - vabatahtlik (*freely given*)
  - konkreetne (*specific*)
  - teadlik (*informed*)
  - ühemõtteline (*unambiguous*)
- Avalduse vormis (*statement*) või selge nõusolekut väljendav tegevus (*clear affirmative action*) → vaikimist, eelnevalt märgistatud lahtreid või tegevusetust ei saa seega pidada nõusolekuks
- Nõusoleku tõendamiskohustus lasub vastutaval töötlejal
- Andmesubjektil õigus nõusolek tagasi võtta, kusjuures nõusoleku tagasivõtmine peab olema sama lihtne kui selle andmine

Andmesubjekti õigused

- Õigus olla informeeritud ja tutvuda andmetega (Art 12-15)
- Õigus andmete parandamisele (Art 16)
- Õigus andmete kustutamisele („õigus olla unustatud“) (Art 17)
- Õigus isikuandmete töötlemise piiramisele (Art 18)
- Andmete ülekandmise õigus (Art 20)
- Õigus esitada vastuväiteid (Art 21)
- Õigus, et isiku kohta ei võetaks vastu otsust, mis põhineb üksnes automatiseeritud töötlusel, sh profiilianalüüsil (Art 22)

Isikuandmete töötlemine teadusuuringu läbiviimisel (Art 89)

- Praegu 3 võimalust:
  1) isiku nõusolek
  2) umbisikustatud andmete kasutamine
  3) isikuandmete töötlemine AKI loal
- Loamenetlus säilib
- Pseudonümiseerimine vs anonümiseerimine

Andmekaitseametnik (Art 37-39)

- Andmekaitseametnik (andmekaitsespetsialist) tuleb määrata kui:
  - isikuandmeid töötleb avaliku sektori asutus või organ (v.a kohus)
  - töötleja põhitegevuse moodustavad isikuandmete töötlemise toimingud
  - töötleja põhitegevuse moodustab eriliigiliste isikuandmete ulatuslik töötlemine
- Andmekaitseametnik võib olla andmetöötleja koosseisuline töötaja või täita ülesandmeid teenuslepingu alusel
- Andmekaitseametnik on andmekaitsealaseid õigusakte ja tavasid eksperdi tasandil tundev isik, kes abistab ja kontrollib andmetöötlejat määruse täitmisel
- Andmekaitseametnikul peab olema võimalik täita oma kohustusi ja ülesandmeid sõltumatul viisil

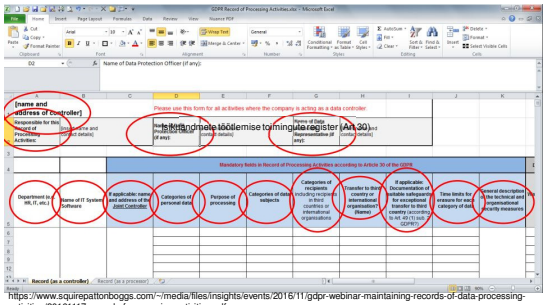
Vaikimisi ja lõimitud andmekaitse (Artikkel 25)

- Lõimitud andmekaitse (*privacy by design*) – uus kohustus eesmärgiga uute süsteemide ja protsesside loomisel arvestada andmekaitsenõuetega, rakendades selleks asjakohaseid tehnilisi ja korralduslikke meetmeid. Andmekaitse kui süsteemi või protsessi ülesehituse osa.
- Vaikimisi andmekaitse (*privacy by default*) – vaikimisi tuleks töödelda ainult neid isikuandmeid, mis on vajalikud töötlemise konkreetse eesmärgi saavutamiseks.

Andmekaitsealane mõjuhinnang (Art 35)

- Kohustus koostada enne isikuandmete töötlemist mõjuhinnang (*data protection impact assessment*), kui töötlemisega kaasneb füüsiliste isikute õigustele ja vabadustele tõenäoliselt suur oht
- Mõjuhinnang on nõutav:
  - ulatuslik automaatne isikuandmete töötlemine
  - delikaatsete isikuandmete ulatuslik töötlemine
- Mõjuhinnang peab sisaldama:
  - Kavandatavate töötlemistoimingute kirjeldus
  - Toimingute vajalikkuse ja proportsionaalsuse hinnang
  - Riskid andmesubjekti õigustele
  - Meetmed riskide maandamiseks

Isikuandmete töötlemise toimingute register (Art 30)



https://www.squirepattonboggs.com/~/media/files/insights/events/2016/11/gdpr-webinar-maintaining-records-of-data-processing-activities/20161117-record-of-processing-activities.pdf

Isikuandmete kaitse ja otseturundus

- Vt ka Elektroonilise side seadus + e-privaatsuse direktiiv
- GDPR põhjenduspunkt 47: Isikuandmete töötlemist otseturunduse eesmärgil võib lugeda õigustatud huviga töötlemiseks.
- Aga ESS § § 103'. Elektrooniliste kontaktandmete kasutamine otseturustuseks:
  - Eelnev nõusolek
  - Või ostjale samasuguste toodete või teenuste otseturustuseks kui:

    1) võimalus andmete esmasel kogumisel keelata selline andmete kasutamine;

    2) võimalus edaspidi alati keelata selline andmete kasutamine;

    3) võimalus keelata elektroonilise side võrgu kaudu.

Järelevalve isikuandmete töötlemise nõuete täitmise üle

- Igas liikmesriigis peab olema sõltumatu järelevalveasutus.
- Eestis on selliseks asutuseks Andmekaitse Inspektsioon (AKI)
- Isikuandmete töötlemise nõuete rikkumise korral on järelevalveasutusel õigus kasutada mitmeid sunnimeetmeid (Art 58), sh:
  - hoiatus
  - noomitus
  - korraldus puuduste kõrvaldamiseks
  - töötlemise piirangute kehtestamine
- Lisaks nimetatud sunnimeetmetele või nende asemele on õigus määrata rahalisi sanktsioone – trahve (Art 83)

Trahvid

- Võrreldes kehtivate trahvimääradega muutuvad summad oluliselt kõrgemaks
- Trahvi saab määrata nii tahtliku rikkumise kui hooletuse puhul
- Rikkumise kategooriad ja trahvimäärad:
  1) Nõ kergemad rikkumised – kuni 10 miljonit eurot või kuni 2% ettevõtte ülemaailmsest aastakäibest (sõltuvalt kumb on suurem)
  2) Nõ raskemad rikkumised – kuni 20 miljonit eurot või kuni 4% ettevõtte ülemaailmsest aastakäibest
- Eestis väärteomenetlus

Andmesubjekti kaebeõigus – õigus tõhusale õiguskaitsele

- Õigus esitada kaebus järelevalveasutusele, kui ta leiab, et tema andmekaitsealaseid õigusi on rikutud (Art 77)
- Õigus pöörduda kohtusse järelevalveasutuse tegevuse või otsuse peale (Art 78)
- Õigus pöörduda kohtusse vastutava või volitatud töötleja vastu, kui ta leiab, et tema andmekaitsealaseid õigusi on rikutud (Art 79)
- Õigus nõuda vastutavalt töötlejalt või volitatud töötlejalt andmekaitsealaste õiguste rikkumisega põhjustatud materiaalse ja mittemateriaalse kahju hüvitamist (Art 82)

Praktiline arutelu

Diskussioon

Helistab väga viisakas vanem meesterahvas ja räägib, et tema lapselaps alustas juba viis aastat tagasi ülikoolis õpinguid, aga tema teada pole veel siiamaani lõpetanud. Ja palutakse öelda, kas tema lapselaps ikka õpib veel ülikoolis või mitte. Ja kui õpib, siis millal ta ükskord lõpetab?

Kuidas käitute?

Variant 1: Kas lahendus oleks teine, kui pöördumine tuleks näiteks meili teel ja see oleks digitaalselt allkirjastatud?

Variant 2: Kas olukord muutub, kui küsijaks oleks üliõpilase ema, kes maksab üliõpilase õpingute eest?

Variant 3: Kas olukord muutub, kui küsijaks on ülikooli töötaja?

Diskussioon

Üliõpilane pöördub õppejõu poole sooviga, et viimane juhendaks tema bakalaureuse tööd. Enne otsuse tegemist vaatab õppejõud ÕIS-ist kõiki selle üliõpilase kohta sinna sisestatud andmeid, sh õpitulemusi ning guugeldab üliõpilast.

Kas õppejõud käitus õigesti?

Diskussioon

Ülikooli rektor käib välja mõtte paigaldada auditooriumitesse videokaamerad, et tagada inimeste ja vara turvalisus ning teostada järelevalvet õpetamise üle. Ülikooli rektor küsib teie arvamust, et kas üldse või millistel tingimusel see on lubatud.

Millist nõu annate?

Diskussioon

Teie hea sõber küsib teilt teie kolleegi mobiiltelefoni numbrit.

Kuidas käitute?

Diskussioon

ÕIS-is sisalduvad üliõpilaste kontaktandmed, sh e-maili aadressid. Vahetult enne lõpetamisi küsib vilistlastegevusega tegelev töötaja ÕISi administraatorilt lõpetavate üliõpilaste e-maili aadressid ja saadab neile kirja koos õnnitlussoovidega ülikooli lõpetamise puhul. Ühtlasi tutvustab vilistlasportaali ja kutsub sellega liituma.

Kas antud juhul on käitutud korrektselt?

Diskussioon

TÜ õppeosakonna poole pöördub organisatsioon, kes palub kinnitada üliõpilasele väljastatud diplomi andmeid, kuna vilistlane kandideerib neile tööle. Vilistlase sellekohane nõusolek puudub.

Kuidas käitute?

Diskussioon

Üliõpilane Mari Maasikas helistab ÕIS-i administraatorile ja soovib teada, kes ja mis eesmärgil on tema andmeid ÕIS-is töödelnud. ÕIS-i administraator keeldub viisakalt ja palub kas isiklikult kohale tulla või saata digiallkirjastatud soov meilile. Mari Maasikas saab väga pahaseks, kuna leiab, et temal on õigus oma andmetega tutvuda ja lubab kaevata Andmekaitse Inspektsioonile.

Kas ÕISi administraator käitus õigesti?

Diskussioon

Bakalaureusetöö raames soovitakse teha uuringut üliõpilaste ülikoolist väljalangemise põhjustest. Uuringus osalemine on isikutele vabatahtlik. Selleks, et isikuid uuringus osalema kutsuda, kasutatakse ÕIS-is olevaid andmeid, sh kontaktandmeid. Valimisse sattunud Kati M. on pahane ja nõuab ülikoolilt vastust, miks ülikool töötleb tema isikuandmeid ilma tema nõusolekuta. Ülikool aga leiab, et kuna isik võib vabalt ise otsustada, kas ta osaleb uuringus või mitte, siis tema tegevus on igati seadustega kooskõlas, pealegi töödeldakse isikuandmeid teadustöö tegemise raames ja selleks ei ole vaja üldse mingit isiku nõusolekut.

Kellel on õigus?

Diskussioon

Kaarel Kask osales TÜ teaduskooli korraldatud emakeele olümpiaadil. Mõni aeg hiljem avastab ta, et FB-s on ülikooli kontol väljas emakeele olümpiaadil tehtud pildid, paaril neist ka tema. Kaarel pöördub teaduskooli poole ja palub need pildid eemaldada. Teaduskool ei ole nõus, kuna leiab, et nende korraldatud ürituste jäädvustamine on juba pika traditsiooniga ning see aitab tutvustada nende tegevusi avalikkusele.

Kas teaduskool tegutses õigesti?

Variant B: Kas vastus oleks teine, kui info pildistamisest, selle eesmärgist ja piltide avalikustamisest oleks kirjas näiteks olümpiaadi kirjelduses/tutvustuses?

Diskussioon

Mati Karu loeb siseveebist uudist, et ülikool hakkab töötajate kontaktide juures kuvama nii sise- kui ka välisveebis töötajate pilte. Selleks kasutatakse pilte, mis on tehtud töötajast töötõendi jaoks. Matile aga üldse tema töötõendi pilt ei meeldi ja ta ei soovi selle avalikustamist.

Kas arvestate Mati sooviga mitte avalikustada tema töötõendi jaoks tehtud pilti?

Diskussioon

Lõpetamise eel küsib vald/linn TÜ-lt oma elanikest lõpetajate andmeid, eesmärgiga avaldada neile tunnustust.

Kuidas käitute?

Diskussioon

Välisriigi saatkond pöördub TÜ poole ja küsib oma riigist pärit õppijate andmeid (nimi, valdkond, õppeaste).

Kas väljastate õppijate andmed?

Diskussioon

TÜ doktorikool tahab atraktiivsuse huvides panna oma kodulehele üles doktorikooli doktorantide nimekirja koos nende lõputööde teemadega.

Millist nõu doktorikoolile annate?

TGS BALTIC
VARUL GRUNTE SUTKIENE

Tänud kuulamast ja kaasa mõtlemast!

Anu Sander
Vandeadvokaat
anu.sander@tgsbaltic.com

Kärt Raud
Advokaat
kart.raud@tgsbaltic.com