TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Mari-Lii Piiskop

ANDMESUBJEKTI ISIKUANDMETE TÖÖTLEMINE NÕUSOLEKU ALUSEL

Magistritöö

Juhendaja
LL.M Mari Männiko
Kaasjuhendaja
dr. iur. Mario Rosentau

Tallinn
2018

SISUKORD

SISSEJUHATUS

Andmekaitse on tänapäeval üks olulisemaid inimõigusi. Viimastel aastakümnetel on uute tehnoloogiliste arengutega see õigus üha vähem kaitstum. Vastuseks neile väljakutsetele on eri maailmaosades rakendatud isikuandmete kaitse seadusi alates 1980. aastast. Seadustel on raske sammu pidada tehnoloogia järjest lühenevate arendustsüklitega. See probleem on peamiselt esile tõusnud internetis, kus on küsitav, kas Euroopa Liidu väide "*Igal indiviidil on õigus teda puudutavate andmete kaitsele"* on endiselt kehtiv? Kas internetikasutajatel on kontroll oma isikuandmete üle, kaasa arvatud selle üle, kuidas neid andmeid kogutakse, hoitakse, töödeldakse, kasutatakse ja avaldatakse?[1]

Euroopa Liidu põhiõiguste harta artikkel 8 tunnustab andmesubjekti nõusolekut kui viisi, kuidas andmesubjektid saavad kaitsta oma isikuandmeid: „*Igaühel on õigus isikuandmete kaitsele. Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Andmeid peab kasutama vaid välja toodud eesmärkidel, kasutades andmetöötluse aluseks andmesubjekti nõusolekut või mõnda muud seadusest tulenevat alust*."[2] Osades Euroopa Liidu liikmesriikides on keerulisem oma andmekaitsealaseid õigusi kasutada (sh interneti kontekstis), sest õigusaktidest tulenevad mitmed ebakõlad. Andmesubjektid on kaotanud kontrolli oma isikuandmete üle. See tuleneb suurtest andmemahtudest, mida igapäevaselt jagatakse. Samuti pole tihti inimesed teadlikud, et neilt andmeid kogutakse. Kuigi paljud eurooplased peavad isikuandmete jagamist üha suuremaks osaks tänapäevasest igapäevaelust, muretseb 72% eurooplastest endiselt, et neilt küsitakse veebis liiga palju personaalset infot. Samuti ei teata, kuidas oma õiguste eest internetis seista.[3] Arvestades viimast skandaali seoses sotsiaalvõrgustikuga *Facebook*, ei saa andmesubjektid kindlad olla, mida nende isikuandmetega pärast nõusoleku linnukese andmist tehakse.[4]

---

[1] United Nations Educational, Scientific and Cultural Organization. Global Survey on Internet Privacy and Freedom of Expression. – UNESCO Publishing 2012.

[2]Euroopa Liidu põhiõiguste harta. - ELT C 326/02 2012. Kättesaadav arvutivõrgus: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:et:PDF.

[3] European Commission. Commission Staff Working Paper. Executive Summary of the Impact Assessment. – Brussels 2012.

[4] S. Bodoni. Facebook Scandal a 'Game Changer' in Data Privacy Regulation. – Bloomberg 08.04.2018. Kättesaadav arvutivõrgus: https://www.bloomberg.com/news/articles/2018–04–07/facebook–scandal–a–game–changer–in–data–privacy–regulation?utm_campaign=socialflow–organic&utm_source=facebook&cmpid=socialflow-facebook-business&utm_medium=social&utm_content=business.

2018. aasta 25. mail hakatakse kohaldama Euroopa Liidus isikuandmete kaitse üldmäärust, mis sätestab mitmeid täpseid kriteeriumeid isikuandmete töötlemiseks. Üldmääruse artikli 6 alusel on isikuandmete töötlemise seaduslikeks alusteks nõusolek, lepingu sõlmimise ning täitmise vajalikkus, juriidilise kohustuse täitmine, füüsiliste isikute eluliste huvide kaitsmine, avaliku võimu teostamine, õigustatud huvi. Käesolevas magistritöös analüüsitakse nõusoleku alusel isikuandmete töötlemist üldmääruse ja hetkel kehtivate sätete kohaselt. Olen valinud konkreetsed valdkonnad, kus on tekkinud kõige suuremad vastuolud isikuandmete töötlemisel nõusoleku alusel. Teema olulisust ja aktuaalsust näitab asjakohaste publikatsioonide arv ning meediakajastus.

Käesoleva magistritöö eesmärk seisneb andmesubjekti nõusolekule kohalduvate nõuete ja probleemide väljaselgitamises uue isikuandmete kaitse üldmääruse ning hetkel kehtiva regulatsiooni kohaselt.

Eesmärgi saavutamiseks püstitan magistritöös järgmised ülesanded:

1) tuua välja andmesubjekti nõusolekule kohalduvad põhimõtted/nõuded ning analüüsida neid tuginedes erinevatele õigusregulatsioonidele ning publikatsioonidele;

2) tuua välja andmesubjekti nõusoleku valdkonnas esinevad probleemid ning analüüsida neid isikuandmete kaitse üldmääruse, õigusaktide ja publikatsioonide kohaselt.

Magistritöö hüpoteesideks on:

1. isikuandmete kaitse üldmääruses sätestatud ning töös analüüsitud nõuded andmesubjekti nõusolekule ei ole normi rakendamiseks piisavalt õigusselged;
2. isikuandmete kaitse üldmääruse nõuded andmetöötluse nõusolekule riivavad ebaproportsionaalselt lapse informatsioonilist enesemääramisõigust infoühiskonna teenuste kasutamisel;
3. nõusolekule kohalduvad nõuded isikuandmete töötlemisel ei taga andmesubjekti informatsioonilist enesemääramisõigust asjakohastes valdkondades.

Magistritöö koosneb kahest peatükist, mis omakorda jagunevad alapeatükkideks. Esimeses peatükis käsitleb autor peamiselt andmesubjekti nõusoleku käsitlust andmekaitsedirektiivi, hetkel kehtiva isikuandmete kaitse seaduse, isikuandmete kaitse seaduse eelnõu ning selle seletuskirja ja isikuandmete kaitse üldmääruse kohaselt. Samuti on olulisel kohal andmesubjekti nõusolekule kohalduvate põhimõtete analüüs ja nõusoleku tõendamiskohustus.

Esile on toodud informatsioonilise enesemääramisõiguse käsitlus nõusoleku andmisel töösuhtes.

Teises peatükis analüüsib autor nõusoleku tähtsust andmete ülekandmisel, teadustööde tegemisel, lapse puhul infoühiskonna teenuste kasutamisel ning kohtupraktikas.

Töö eesmärkide saavutamiseks on autor kasutanud peamiselt analüütilist meetodit, sest see on kõige sobivam meetod asjakohaste probleemide lahendamiseks. Magistritöö autori hinnangul on eestikeelset magistritöö teemat käsitlevat õiguskirjandust vähe. Valdavalt on materjal võõrkeelne (viimastel aastatel kirjutatud teadusartiklid). Magistritöö kirjutamisel tugines autor Eesti ja Euroopa Liidu õigusaktidele, Euroopa Liidu institutsioonide materjalidele, Andmekaitse Inspektsiooni juhistele, asjakohasele erialakirjandusele ning ka Euroopa Liidu Kohtu praktikale ja Euroopa Inimõiguste Kohtu lahenditele.

Magistritööd iseloomustavad märksõnad on andmekaitse, nõusolek, isikuandmete kaitse üldmäärus, informatsiooniline enesemääramisõigus.

Autor tänab oma juhendajaid Mari Männikot ja Mario Rosentaud magistritöö kirjutamisel antud väärtuslike nõuannete eest.

1. ANDMESUBJEKTI NÕUSOLEK ANDMEKAITSEÕIGUSES

1.1. Isikuandmete kaitse regulatsioon Euroopa Liidus ja Eestis

1.1.1. Andmekaitsedirektiiv 95/46/EÜ

Andmesubjekti nõusolek on olnud üheks olulisemaks aluseks isikuandmete töötlemisel andmekaitseõiguses. Eurobaromeetri andmekaitsealases uuringus vastas 69% küsitletutest, et nende isikuandmete töötlemiseks ja kogumiseks peaks olema küsitud selgesõnaline nõusolek kõikidel juhtudel. 14% küsitletutest vastas, et veebiteenuste pakkumisel peaks küsima nende nõusolekut isikuandmete töötlemiseks.[5]

Nõusolek on enamikel juhtudel olnud andmetöötluse aluseks ning üheks tähtsaimaks kaitsemeetmeks isiku privaatsusõiguse puhul. Isikuandmete kaitse üldmääruse eelkäijaks oli 1995. aastal vastu võetud andmekaitsedirektiiv, mis samuti selgitas ning täpsustas nõusoleku olemust. Direktiivi (nagu ka üldmääruse) eesmärgiks oli andmekaitseseaduste harmoniseerimine kõikides Euroopa Liidu liikmesriikides.[6] Andmesubjekti nõusolek on direktiivi artiklis 2 lõikes h defineeritud järgnevalt: „*Iga vabatahtlik, konkreetne ja teadlik tahteavaldus, millega andmesubjekt annab nõusoleku töödelda tema kohta käivaid andmeid*“.[7] Eelkõige on direktiivis olnud olulisel kohal, et nõusolek oleks antud enne andmete töötlemist ning et see peaks olema ühemõtteline. Nõusoleku ühemõttelisust sisustati andmekaitsedirektiivi selgitustes järgnevalt: andmetöötlejal ei tohiks jääda mitte mingisugust kahtlust isiku nõusoleku kehtivuse osas ning see peab olema selge. Samuti on andmetöötlejal kohustus tuvastada isik, kui nõusolek antakse kas telefoni teel või veebikeskkonnas.[8]

Direktiivis on mitmed põhimõtted kirjeldatud, mis on edasiarendatud kujul üldmääruses olemas: näiteks on ka direktiivis täpsustatud eriliigiliste isikuandmete töötlemist, nõusoleku selgesõnalisuse põhimõtet ning definitsiooni.[9] Direktiivi mõttes on nõusolek õiguslik vahend, mis annab isikule võimaluse kontrollida oma isikuandmeid ning mõelda selle üle, kellele andmeid edastada ning kellele mitte. Direktiiv on selles osas sarnane isikuandmete kaitse üldmäärusega.[10] Nõusoleku põhimõtted ja rakendamine on olnud direktiivis oluline tööriist

[5] European Commission. Data Protection. Report. – Special Eurobarometer 431 2015, page 58. Kättesaadav arvutivõrgus: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf.
[6] European Union Agency for Fundamental Rights. Council of Europe. Handbook on European data protection law 2014. Kättesaadav arvutivõrgus: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.
[7] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. Kättesaadav arvutivõrgus: http://eurlex.europa.eu/legalcontent/et/ALL/?uri=CELEX:31995L0046.
[8] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent. 13.07.2011. Kättesaadav arvutivõrgus: http://www.pdpjournals.com/docs/88081.pdf.
[9] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ.
[10] D. J. Solove. Privacy Self-Management and the Consent Dilemmas. - Harvard Law Review, vol. 126, 2014.

ning on ka alustalaks isikuandmete kaitse üldmäärusele, kuid võrreldes 1995. aastaga on infotehnoloogia väga palju edasi arenenud. Direktiiv on tänapäevases kontekstis liiga laialt tõlgendatav ning ebaselge. Kindlasti ei tasuks alahinnata direktiivi tähtsust, sest see pani aluse olulistele printsiipidele, mida on nüüdses üldmääruses edasi arendatud ning täpsustatud. Suureks erinevuseks direktiivi ja üldmääruse puhul on asjaolu, et direktiiv ei ole otsekohalduv ning seetõttu võisid liikmesriigiti tekkida erinevused seadustes. Eestis on direktiiv implementeeritud isikuandmete kaitse seadusega. Üldmäärus on otsekohalduv ning kehtib sellisel kujul kõikides liikmesriikides.

1.1.2. Isikuandmete kaitse üldmäärus

Isikuandmete kaitse üldmäärus (edaspidi: üldmäärus), mida hakatakse kohaldama 25. maist 2018, täpsustab nõusoleku formaalseid ning sisulisi nõudeid. Üldmääruse põhimõteteks on põhjenduspunktides 2 ja 4 kaasajastada andmekaitse nõudeid, austada aluslepingus sätestatud põhimõtteid, tugevdada liikmesriikide majandusalaseid näitajaid ning tagada suuremal määral füüsiliste isikute rahulolu. Samuti on üldmääruse kandvaks ideeks mõte, et isikuandmed kuuluvad andmesubjektile, mitte andmetöötlejale.[11]

Nõusoleku puhul on tähtis märkida, et isik peab aru saama, millele nõusolek antakse. Üldmäärus loob rangemad nõudmised ka selles osas: oluline on määratleda andmesubjekti jaoks andmete liik, mida tema kohta kogutakse ning võimalikult täpselt määratleda eesmärgid. Andmete töötlemine on mitmetel juhtudel lubatud, kui on üldmääruse artikli 4 punkti 11 alusel olemas vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega.[12] Selline põhimõte on otseselt seotud läbipaistvuse põhimõttega, mis on üks Euroopa Liidu andmekaitse alustaladest – nõusolek annab põhilise õigusliku aluse isikuandmete töötlemiseks ja seda on nüüdseks tugevdatud selge nõusoleku nõudega, mis on sätestatud uues üldmääruses.[13] Nõusolek on muutunud üldmääruse kontekstis veelgi olulisemaks ning nõuab kõrgendatud tähelepanu erinevatelt ettevõtetelt, kes peavad kriitiliselt üle vaatama kõik hetkel kehtivad lepingud, nõusolekuankeedid ja muud relevantsed dokumendid.

---

[11] Euroopa Parlamendi ja Nõukogu määrus 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679.

[12] *Ibid.*

[13] S. Montelone. Addressing the Failure of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation. – Syracuse J. Int'l L. & Com. 2015.

Kui analüüsida uudset olukorda andmesubjekti seisukohalt, siis oleks kindlasti vajalik andmesubjekte koolitada, et nad mõistaksid andmekaitse aspekte ning privaatsuspoliitika põhimõtteid paremini. Samuti oleks vaja muuta teavitavaid vorme sellisel määral, et need oleksid rohkem arusaadavamad, selgemad ja konkreetsemad. Sellega võivad kaasneda mitmed rahalised raskused ning õiguskeele lihtsustamine võib põhjustada õiguslikku selgusetust, mis omakorda võib kaasa tuua mitmeti tõlgendatavaid olukordi.[14] Nõustun eeltoodud arvamusega, et õiguskeele lihtsustamine võib kaasa tuua uusi probleeme, kuid samal ajal pakub see lahendust, kuidas paremini selgitada andmesubjektile tema õiguseid ja andmetöötluse eesmärke. Kuna selgitused peavad olema arusaadavad kõigile, siis on äärmiselt vajalik selge ja konkreetne sõnastus. See peaks olema rohkem esile toodud, et andmesubjektil ei jääks oluline info märkamata. Näiteks võib relevantne tekst olla rasvases kirjas ning suurema tähesuurusega kui ülejäänud tekst.

Euroopa Liidu Põhiõiguste Amet on oma uuringus esile toonud, et avalikkust peab rohkem teavitama andmekaitsealastest rikkumistest, nendega seotud õiguskaitsevahenditest ja erinevatest mehhanismidest. Samuti peab alati arvesse võtma, et andmekaitserikkumised võivad põhjustada isikutele psühholoogilist ja sotsiaalset kahju, mis mõjutab andmesubjekte negatiivselt. Seetõttu on oluline, et siseriiklikud andmekaitseasutused tegeleksid rohkem isikute teavitamisega ja keskenduksid nö kaitserollile andmekaitseõiguses.[15] Kahju võib seisneda selles, et isikuandmete kasutamise tõttu käitub inimene erinevalt, st tema vabadus on seetõttu piiratud. Tekkinud võib-olla ka mainekahju või moraalne kahju vaimsete kannatuste tõttu.

Uus üldmäärus loob rohkem kohustusi siseriiklikele andmekaitseasutustele, mis on kindlasti vajalik. See tõhustab järelevalvet era- ja avaliku sektori üle. Samuti on olulisel kohal laiaulatuslik teavitustöö, mis selgitaks paljudele andmesubjektidele andmekaitse olemust, tähtsaid põhimõtteid enda kaitsmise osas ning reaalsete rikkumiste äratundmises.

Üldmääruse kohta on mitmeid artikleid kirjutatud ning erinevaid arvamusi esitatud. Näiteks on P. K. Tupay välja toonud, et õigusaktide uuendamine ei taga veel andmekaitsereformi edukust. Samuti on artiklis välja toodud Kasseli Ülikooli professori Alexander Roßnageli arvamus, et

[14] J. Mišek. Consent to Personal Data Processing. – The Panacea or the dead end? – Masaryk University Journal of Law and Technology 2014.
[15] Euroopa Liidu Põhiõiguste Amet. Juurdepääs andmekaitse õiguskaitsevahenditele Euroopa Liidu liikmesriikides. – Euroopa Liidu Põhiõiguste Ameti väljaannete talitus 2013.

õiguslikku ebakindlust tekitab üldmääruse üldsõnalisus.[16] Üldmäärus on nõusolekule kohalduvate nõuete osas üldsõnaline. Piisavalt selgelt pole välja toodud, kui täpselt peavad olema töötlemise eesmärgid kirjas ning millised lahendused on kõige paremad spetsiifilistes olukordades. Näiteks kuidas lahendada olukorda, kui inimene on andnud nõusoleku oma isikuandmete töötlemiseks taustauuringu tegemiseks, kuid kliendisuhet edasiselt ei teki. Sellisel juhul peab arvestama erinevate seadusest tulenevate nõuetega ja eesmärgikohasuse põhimõttega selles osas, kui kaua peaks isikuandmeid säilitama (ühtset ja kindlat lahendust hetkel ei ole). Samuti tekib suur koormus ettevõtte huvidele olemasolevate nõusolekute uuendamine (kui nõusolek ei vasta üldmääruses sätestatud nõuetele, siis peab selle uuesti küsima[17]). Kui pole võimalik saada nõusolekut, siis sellisel juhul kaasneb automaatne isikuandmete töötlemise lõppemine või peab ettevõtte leidma mõne muu õigusliku aluse. Hetkel on mitmeid aspekte, mis võivad olla mitmeti tõlgendatavad ning vajavad täiendavat analüüsi ettevõtete enda poolt.

Andmete töötlemise puhul on oluline välja selgitada, kas andmetöötluse seaduslikuks aluseks on nõusolek või on selle tegevuse jaoks olemas mõni muu üldmääruses sätestatud alus. Õigusliku aluse leidmisel peab arvestama üldmääruse artikliga 6, mis selgitab andmesubjekti nõusolekut ja teisi võimalusi, mille puhul on võimalik isikuandmeid töödelda. Probleem on ka selles, et regulatsioon ei täpsusta, millal on õige isikuandmeid nõusoleku alusel töödelda ning millal peaks teisi aluseid arvesse võtma. Kohati on üldmääruse üldine mõte lõpetamata ja tükeldatud, mis loob palju tõlgendamisvõimalusi ning ebaselgeid olukordi.[18] Eelkõige peaks üldmäärus tagama suuremal määral andmekaitset ning looma selgemaid ja arusaadavaimaid printsiipe antud valdkonnas, kuid antud juhul on see juurde toonud ka mitmeti tõlgendamisi.

Üldmääruse kohaselt on teatud liiki isikuandmeid, mida on lubatud ainult seaduse alusel või ametiasutuse järelevalve all töödelda. Näiteks on selleks isiku kohta käivad süüteoasjades süüdimõistvad kohtuotsused, mis on sätestatud üldmääruse artiklis 10.[19] Kõik ettevõtted ja tööandjad peaksid läbi mõtlema, milliseid isikuandmeid on neil võimalik töödelda seaduste alusel, õigustatud huvi korral, teatud juhtudel eluliste huvide kaitseks, lepingu sõlmimise/täitmise eesmärgil ja nõusoleku alusel. Andmetöötlejad peaksid olema teadlikud

[16] P. K. Tupay. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. – Juridica IV, 2016.
[17] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 30.
[18] D.W. Schartum. Intelligible Data Protection Legislation: A Procedural Approach. – Oslo Law Review 2017.
[19] Euroopa Parlamendi ja Nõukogu määrus 2016/679.

erinevatest Andmekaitse Töörühma juhistest, siseriiklikest muudatustest ja tulevikus ka kohtulahenditest, mis saavad olema sätete tõlgendamisel tähtsaks abiks ja suunanäitajaks.

1.1.3. Eesti isikuandmete kaitse seadus, uue isikuandmete kaitse seaduse eelnõu ja seletuskiri

Nõusoleku olemust on defineeritud ka isikuandmete kaitse seaduses. Näiteks on isikuandmete kaitse seaduse (edaspidi: IKS) §-s 6 sätestatud isikuandmete töötlemise põhimõtted ja üheks olulisemaks on lõikes 4 kirjeldatud kasutuse piiramise põhimõte – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal ning § 10 lõikes 1 on kirjas põhimõte, et isikuandmete töötlemine on lubatud üksnes andmesubjekti nõusolekul, kui seadus ei sätesta teisiti. IKS täpsustab nõusoleku olemust §-s 12, kus on lõikes 1 kirjas, et nõusolek peab põhinema vabal tahtel ning lõige 7 täpsustab, et nõusoleku võib igal ajal tagasi võtta. Samuti on §-s 7 kirjas nõusoleku vorm ning ka teised printsiibid, mis on mingil määral kooskõlas uue isikuandmete kaitse üldmäärusega.[20] Eestis on kehtinud konkreetne ja selge isikuandmete kaitse seadus, mis on siiani sisustanud nõusoleku olemust.

Uue isikuandmete kaitse seaduse eelnõu mitmed sätted täpsustavad nõusoleku tingimusi. Näiteks on IKS eelnõu §-s 4 sätestatud isikuandmete töötlemine ajakirjanduslikul eesmärgil, §-s 6 on välja toodud erisus teadusuuringute, ajaloouuringute ja riikliku statistika puhul. Seadus rakendusaktina on täpsustanud nüansse, mida üldmäärus nii täpselt ei reguleeri.[21] Võrdlusena võib tuua näite üldmääruse rakendamisest Saksamaalt, sest Saksamaa on andmekaitsevaldkonnas eeskujuks mitmetele riikidele ning Saksamaa õigussüsteem on sarnane Eesti omale. Saksamaa föderaalse andmekaitse seaduse § 26 lg 2 kehtestab tööandjale konkreetsemad nõusoleku andmise kohta käivad tingimused: „*Kui töötaja isikuandmeid töödeldakse nõusoleku alusel, arvestatakse seda, kas selline nõusolek oli vabatahtlik, hinnates töötaja sõltuvust töösuhtes ja nõusoleku andmise tingimused. Nõusolekut võib anda vabatahtlikult, kui see on seotud töötaja õigusliku või majandusliku eelisega või kui tööandja ja töötaja järgivad samu huve. Nõusolek antakse kirjalikult, välja arvatud juhul, kui eriolukorra tõttu on asjakohane teistsugune vorm*“.[22] Eestis on AKI eelnõule avaldatud arvamuses välja toonud, et töösuhte kontekstis peaks ära reguleerima jälgimisseadmestike (töökorralduslikud

[20] Isikuandmete kaitse seadus. – RT I, 06.01.2016, 10
[21] Isikuandmete kaitse seaduse eelnõu. 21.03.2018. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_en.21.03.18.pdf.
[22] The Bundestag. Federal Data Protection Act. Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 30.06.2017. Kättesaadav arvutivõrgus: https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf.

kaamerad, turvakaamerad, GPS-seadmed, arvutiprogrammid töötajate tegevuse kontrollimiseks jne) kasutamise.[23] Saksamaa on konkreetselt sätestanud, et nõusolek töösuhtes peab olema antud kirjalikult (v.a kui on tegemist eriolukorraga). Samuti on täpsemalt välja toodud, mis olukorras saab lugeda nõusolekut vabatahtlikult antuks. Määruse artikkel 88 annab liikmesriikidele võimaluse töösuhetes täpsustuste esile toomiseks siseriiklikus õiguses.[24] Autori hinnangul oleks sarnase sätte väljatoomine mõistlik ka Eestis: kas sätestada isikuandmete kaitse seadusega või mõne teise relevantse õigusaktiga. Hetkel ei ole erasektori puhul erisust sätestatud isikuandmete kaitse seaduse rakendamise seaduse eelnõus[25] ega isikuandmete kaitse seaduse eelnõus.[26] Saksamaa on lisanud föderaalse andmekaitse seaduse §-i 51 nõusolekule kohalduvad põhimõtted. Eraldi on esile toodud nõusoleku tagasivõtmise õigus, vabatahtlikkuse aspekt, nõusoleku tõendamiskohustus jne.[27] Autori hinnangul pole Eesti isikuandmete kaitse seaduses vaja eelmainitud printsiipe eraldi välja tuua, kuna need on olemas üldmääruses (see tooks kaasa dubleerimise). Olemasolevas eelnõus[28] pole antud põhimõtteid eraldi välja toodud ning osasid printsiipe on selgitatud näidete abil eelnõu seletuskirjas.

Uue isikuandmete kaitse seaduse eelnõu seletuskiri selgitab nõusolekuga seotud olukordi. Seletuskiri põhjendab, et andmesubjekti tuleb informeerida selges ja lihtsas keeles. See puudutab nõusoleku küsimist, teabe esitamist ning andmesubjekti teavitamist rikkumisest.[29] Kehtiv seadus sätestab, et teave tuleb esitada andmesubjektile nõusoleku küsimise ajal või enne seda (IKS § 12 lg-d 1 ja 3), üldmäärus sätestab, et isikuandmete saamise ajal (artikkel 13 lg 1). Seletuskirjas öeldakse, et ei ole võimalik hinnata, kui palju on andmesubjektid seni oma õigusi seoses isikuandmete töötlemisega kasutanud ning kui palju hakatakse neid õigusi kasutama peale üldmääruse kohaldamist.[30] Võib arvata, et inimeste teadlikkus on suurenenud ning ilmselt suureneb aja jooksul veelgi. Seetõttu on oluline üldmääruse kohta rohkem infot levitada ja inimesi harida. Autor on arvamusel, et alates uue üldmääruse rakendamisest hakkavad inimesed andmekaitsele rohkem tähelepanu pöörama ja oma õiguste eest seisma. Osaliselt võib see olla ka seetõttu, et meedia on teemale palju tähelepanu pööranud ning kindlasti aitavad kaasa

[23] Andmekaitse Inspektsioon. IKS eelnõule arvamuse avaldamine 21.12.2017. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/eelnoule_arvamuse_avaldamine_-_uus_iks.pdf.
[24] Euroopa Parlamendi ja Nõukogu määrus 2016/679.
[25] Isikuandmete kaitse seaduse rakendamise seaduse eelnõu. 15.03.2018. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_rs_en.pdf.
[26] Isikuandmete kaitse seaduse eelnõu. 21.03.2018.
[27] The Bundestag. Federal Data Protection Act.
[28] Isikuandmete kaitse seaduse eelnõu. 21.03.2018.
[29] Isikuandmete kaitse seaduse eelnõu seletuskiri. 21.03.2018, lk 54. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_sk_21.03.18.pdf.
[30] *Ibid*, lk 51.

üldmääruses sätestatud erinevad andmesubjektide teavitamiskohustused.

1.2. Andmesubjekti nõusoleku olulised põhimõtted

1.2.1. Informatsiooniline enesemääramisõigus

Nõusoleku andmine andmekaitseõiguses ning informatsiooniline enesemääramine on olulisel määral omavahel seotud. Informatsioonilise enesemääramisõiguse puhul on vajalik selgitada mõiste tähendust ning seotust nõusolekuga andmekaitseõiguses.

Termin „informatsiooniline enesemääramisõigus" pärineb Saksamaalt ning on tänaseks levinud ka teistesse Euroopa riikidesse. Saksa Föderaalkohus asus seisukohale, et tulenevalt põhiseadusest on igaühel õigus ise määrata, kellele oma isikuandmeid üle anda. Informatsioonilise enesemääramisõiguse piirangud on lubatud ainult ülekaaluka üldise huvi korral. Piirangud peavad tulenema seadusest ning asjakohased normid peavad olema õigusriigile omaselt selgelt ja konkreetselt sätestatud. Informatsioonilise enesemääramisõiguse kaitsmine ongi oluline isikuandmete kaitse eesmärk.[31] Saksa kohtusüsteem on võtnud endale kohustuse hinnata informatsioonilist enesemääramist, tasakaalustades seda teiste huvidega. Kuigi see lähenemine võimaldab kohtunikel teha suulisi valikuid konfliktide lahendamiseks, ei anna see väärtuste skaalal piisavalt kaalu huvide kindlakstegemiseks.[32] Poola põhiseadus tunnustab selgesõnaliselt õigust enesemääramisele isikliku õiguse kujul ehk õigust „otsustada oma isikliku elu üle", mida mainitakse samas sättes koos üldise õigusega era- ja perekonnaelule. Üldisemalt on ka Saksa põhiseadus kehtestanud isiku õiguse oma isiksuse vabale kujunemisele. See on laiem kui eraelu puutumatus, kuid on olnud informatsioonilise enesemääramisõiguse peamise põhiseadusliku ilmingu aluseks.[33] Võib veel ka lisada, et Euroopa Liidu põhiõiguste hartas ei ole küll artiklis 8 (isikuandmete kaitse) selgesõnaliselt informatsioonilist enesemääramisõigust välja toodud, kuid harta eelnõudel oli algselt suurem rõhuasetus informatsioonilise enesemääramise mõistel. Näiteks 5. mai 2000. aasta harta eelnõu artikkel 19 nägi ette, et *„Kõigil on õigus ise otsustada, kas tema isikuandmeid võib avalikustada ja kuidas neid kasutada"*. Harta teksti sõnastuse hilinenud muutust võib seletada mitme teguriga. Näiteks võisid tekstide autorid „informatsioonilist enesemääramist" tajuda nii, et see oli Saksamaa

[31] Andmekaitse Inspektsioon. Ettekanne Riigikogule 2003. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/2003.rtf, 21.02.2018.
[32] P. Schwartz. The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination. – The American Journal of Comparative Law 1989.
[33] B. Koops, B. Clayton Newell, T. Timan, I. Skorvanek, T. Chokrevski, M. Galic. A Typology of Privacy. – University of Pennsylvania Journal of International Law 2016.

õiguskorrale lähemal, kui see oli asjakohane EL-i pluralistlikus õiguskorras.[34] Seega võib väita, et Saksamaa on olnud oluliseks informatsioonilise enesemääramisõiguse loojaks ning edasiarendajaks. See on kaasa toonud olukorra, kus antud õigus on muutunud tähtsaks ka teistes Euroopa Liidu liikmesriikides.

Eesti põhiseaduse kommentaarides on selgitatud, et informatsiooniline enesemääramine tähendab igaühe õigust ise otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse, seetõttu on üheks oluliseks valdkonnaks isikuandmete kaitse.[35] Õigusteadlane Robert Alexy on väitnud, et informatsiooniline enesemääramisõigus on moodsa andmetöötluse tingimustes eriti tähtis. Isegi suhteliselt tähtsusetute andmete kaudu võib elektroonilise andmetöötluse abil väga kergesti ja palju isiku kohta teada saada.[36] Kindlasti peab rõhutama, et informatsiooniline enesemääramisõigus on tänapäeval muutunud, sest isikul ei ole enda kohta internetis olnud ja olevate andmete töötlemise üle lõplikku kontrolli.[37] Samal ajal on oluline välja tuua, et kontroll saab realiseeruda ainult juhul, kui isik on teadlik tema kohta käivate andmete kogumisest.[38]

Kuna isikuandmete kaitse õigust pole eraldi põhiseaduses sätestatud, siis on olulisel kohal eraelu puutumatus, mille alla isikuandmete kaitse läheb. Riigikohtu halduskolleegium on märkinud, et eraelu puutumatuse riivena käsitletakse isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist.[39] Samuti on Riigikohtu kriminaalkolleegium väitnud, et inimkeskses ühiskonnas tohib põhiõiguste konfliktolukordades kõige vähem piirata inimväärikust - kompleksset põhiõigust, mille elementideks on eeskätt õigus heale nimele, õigus mitte olla hirmul enese ja oma lähedaste eksistentsi pärast, õigus õiguslikule võrdsusele kõigi teiste inimestega, õigus inimlikule identiteedile, õigus informatsioonilisele enesemääramisele, õigus kehalisele puutumatusele.[40] Seega võib väita, et informatsiooniline enesemääramisõigus on ka Eesti kohtusüsteemis olulisel kohal ning seda õigust väärtustatakse kõrgelt.

---

[34] O. Lynskey. Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order. – International and Comparative Law Quarterly 2014.
[35] Ü. Madise jt. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. PS kommentaarid § 26 komm 24. – Tallinn. Kättesaadav arvutivõrgus:http://www.pohiseadus.ee/index.php?sid=1&pt=&p=26#c24.
[36] R. Alexy. Põhiõigused Eesti põhiseaduses. - Justiitsministeerium. Põhiseaduse juriidilise ekspertiisi komisjon 1997. Kättesaadav arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/elfinder/article_files/prof_robert_alexy._pohioigused_eesti_pohiseaduses.pdf.
[37] M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Kirjastus Juura 2011, lk 185.
[38] M. Rondel. Informatsioonilise enesemääramise õigus ja jälitustegevus. – Juridica X, 2016.
[39] RKHKo 3-3-1-3-12 p 19.
[40] RKKKo 3-1-1-80-97 p 1.

Tähtis on tunnustada andmekaitset kui eraldiseisvat õigust, suurendades seeläbi juurdepääsu informatsioonilisele enesemääramisele ja ennetades võimude asümmeetriat. Selleks, et eraelu puutumatuse ja andmekaitse vahelist potentsiaalset pinget leevendada, peab olema selge, millised on täpsed andmekaitse väärtused ühiskonnale ja demokraatiale.[41] Oluline on ka rõhutada, et informatsioonilise enesemääramisõiguse kontseptsioon seab fookusesse inimese enda otsustusõiguse ja vastutuse. Keegi teine ei kaitse ega tee otsustusi, mida inimene pärast kritiseerida saaks.[42]

Infoühiskonnast tulenevad väljakutsed ähvardavad inimeste võimet arutleda ja teha õigeid valikuid nendega seotud asjades. Informatsiooniline enesemääramine on tarvilik tervikliku isiksuse arengu ja kodanike osaluse suurendamiseks ühiskondlikel teemadel. Vajalik on tagada, et seadus oleks üles ehitatud sellisel kujul, mis säilitaks indiviidi võimet vabalt otsuseid langetada. Tähtis on rakendada ettevaatusabinõusid, et tagada inimeste võimekust end informatsiooniliselt määrata.[43] Näitena võib tuua, et Euroopa Liidu õigus aitab üksikisikutel aktiivsemalt kontrollida, milline teave on edastatud kolmandatele isikutele, samal ajal kui Ameerika Ühendriikide seadused kaitsevad suhteliselt passiivselt andmesubjekti andmete edastamise osas.[44]

Andmekaitse ei ole küll informatsioonilise enesemääramise sünonüüm, kuid ta on tihedalt sellega seotud. Informatsioonilise enesemääramise perspektiiv on olulisel määral mõjutanud andmekaitse arengut. Andmekaitsealastes diskussioonides toetavad mõningad informatsioonilise enesemääramise radikaalsemaid vorme kui teised, kuid millises maailmas elavad inimesed, kes väidavad, et üksikisikud saavad oma isikuandmeid kontrollida?[45] Seoses informatsioonilise enesemääramisega on esile toodud, et üldmääruse nõuded ei muuda andmesubjekti õiguslikku positsiooni kindlamaks. See võib luua illusiooni, et andmesubjekt suudab jälgida enda huvisid ja privaatsust, mis ei pruugi tuua loodetud tulemust.[46] Praeguste mudelite täiustamine ja nende alusel saadud nõusoleku andmise protseduur ei pruugi olla piisav, et tagada sotsiaalmeedia kasutajate privaatsus, nende eraelu puutumatus ning ka nõusoleku

[41] A. Forde.The Conceptual Relationship between Privacy and Data Protection. – Cambridge Law Review 2016.
[42] H. Harro-Loit. Informatsiooniline enesemääramine kui üks teabekeskkonnas toimetuleku võtmekontseptsioonidest. – Tartu Ülikooli haridusuuringute ja õppekavaarenduse keskus 2010, lk 109. Kättesaadav arvutivõrgus: https://dspace.ut.ee/bitstream/handle/10062/40923/Uld_Oppekavad1.pdf?sequence=1.
[43] E. J. Eberle. The Right to Information Self-Determination. – Utah Law Review 2001.
[44] A. Suuberg. The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law. - Tulane Journal of Technology and Intellectual Property 2013.
[45] B. Koops. The Trouble with European Data Protection Law. – TILT Law and Technology Preprint Publications 2014.
[46] P. Blume. The Data Subject. – European Data Protection Law Review 2015.

ootused. Kuigi kavandatavate Euroopa Liidu õigusaktide mudelite optimeerimisel on palju valikuid, siis ei tohiks loobuda informatsioonilise enesemääramise kontseptsioonist. Samal ajal oleks vaja täiendavaid uuringuid ka teiste mudelite kohta, mis paremini kajastaksid seda, kuidas inimesed sotsiaalmeediat praktikas kasutavad.[47] Üldmäärus võib kohati tekitada illusiooni, et inimestel on kontroll oma isikuandmete üle, kuid tegelikkuses on siiski võimatu öelda, kas infoühiskonnas on isikuandmete kogumine piisavalt jälgitav ja arusaadav ka tavainimeste jaoks. Seetõttu on kindlasti oluline andmesubjekte võimalikult palju harida ning panna neid mõtlema oma isikuandmete avaldamise mahu ja vajalikkuse osas. Ka töösuhtes võivad tekkida olukorrad, kus isik ei saa end informatsiooniliselt määrata, sest tunneb sundust infot anda. Näiteks on ankeetides palutud lisada info laste kohta, kuid pole täpsustatud, kas info andmine on vabatahtlik või mitte ning mis on selle eesmärk (osadel juhtudel on eesmärgiks jõulupakkide andmine tööandja poolt). Seetõttu on oluline kirje olemasolu, et andmete andmine oleks vabatahtlik ja selle info jagamisest keeldumisele ei järgneks negatiivseid tagajärgi. Vastasel juhul on andmetöötlus vastuolus seaduslikkuse ja õiglase töötlemise põhimõtetega. Informatsiooniline enesemääramisõigus on olulisel kohal ning seotud nõusoleku andmisega suurel määral, sest nõusoleku andmine peaks tagama ka andmesubjekti informatsioonilise enesemääramise.

1.2.2. Nõusoleku vabatahtlikkus ja ühemõttelisus

Üldmääruse põhjenduspunktis 32 rõhutatakse, et andmesubjekt peab andma nõusoleku teda puudutavate isikuandmete töötlemiseks vabatahtlikult, konkreetselt, teadlikult ja ühemõtteliselt. Näitena on samas lõigus toodud, et see võiks hõlmata vajaliku lahtri märgistamist veebisaidil, infoühiskonna tehniliste seadmete valimist või muud avaldust või käitumist, millest selle kontekstis konkreetselt nähtub andmesubjekti nõusolek teda puudutavate isikuandmete kavandatavaks töötlemiseks. Vaikimist või tegevusetust ei tohiks seega pidada nõusolekuks. Oluline on ka eesmärgikohasus, sest kõikide töötlemise eesmärkide kohta peab olema selgitus.[48]

Vabatahtlikkus tähendab eelkõige andmesubjektide tegelikku valikut ja kontrolli. See tähendab ka seda, et ei tohiks jääda mingisugust kahtlust nõusoleku vabatahtlikkuses. Üldmääruse punkt 42 kirjeldab, et kui andmesubjektil puudub tegelik ja vaba valik, ta tunneb end kohustatuna

[47] B. Custers, S. van der Hof, B. Schermer, S. Appleby-Arnold, N. Brockdorff. Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law. – SCRIPTed 2013.
[48] Euroopa Parlamendi ja Nõukogu määrus 2016/679.

nõusolekut andma või kui ta ei saa kahjulike tagajärgedeta nõusoleku andmisest keelduda, siis ei ole isik andnud kehtivat nõusolekut.[49] Sellest tulenevalt ei loeta nõusolekut vabatahtlikuks, kui andmesubjekt ei saa keelduda nõusoleku andmisest või oma nõusolekut tagasi võtta. Näiteks on keeruline määratleda nõusolekut tööandja ja töötaja omavahelises suhtes jälgimisseadmete kasutamisel. Kuna tegemist on alluvussuhtega, siis ei ole nõusolek kehtivaks isikuandmete töötlemise aluseks, sest vabatahtlikkuse aspekt puudub. Töötajat võivad oodata negatiivsed tagajärjed, kui ta nõusolekut ei anna. Nõusoleku sisulisem mõte on, et see ei saa olla antud vabatahtlikult, kui isikut võib keeldumise korral ees oodata mõni oluline negatiivne tagajärg.[50] Töösuhtes ei saa alati põhjendatud aluseks nõusolekut lugeda ning vajalik on määratleda, miks ja mis alusel isikuandmeid töödeldakse. Seetõttu peaks tööalases suhtes olema pigem õiguslikuks aluseks isikuandmete töötlemisel kas seadus või töölepingu täitmine, kuid mitte nõusolek.

Ühe näitena võib veel esile tuua registreerumise sotsiaalmeediakontol – näiteks sotsiaalmeedia platvormi *Facebook*. *Facebook'*i kasutaja loomisel on nõusolek kehtiv alus andmete töötlemiseks, sest andmesubjektil on olemas valik, kas ta kasutab seda teenust või mitte. Kuigi teenusel on väga laialdane kasutus ja suur turuosa ning andmesubjektil võivad esineda negatiivsed tagajärjed (näiteks pole võimalik saada kooliga/tööga seotud vajalikku informatsiooni), siis ei saa teenusest loobumist siiski kirjeldada kui olulist negatiivset efekti.[51] Kui isik otsustab kasutajakontost loobuda, siis see ei ole suur negatiivne efekt, kuid samal ajal piirab selline tagajärg isiku sotsiaalset suhtlust ja info saamist. Andmesubjektid peavad arvestama isikuandmete andmisega, sest teenusepakkujal pole alati võimalik korrektselt teenust pakkuda ilma nõusolekuta ning isikuandmeteta. *Facebooki* kasutamistingimuste punktis 2 on kirjas, et kui isik postitab avalikku striimi avalike seadete alt, siis on postitatu (näiteks nimi ja profiilipilt) kõigile vabalt kasutatav.[52] Seega on antud blanko nõusolek loetlemata isikute ringile, kes võivad isikuandmeid töödelda erinevatel eesmärkidel, mis ei sõltu üldse andmesubjektist. See loob olukorra, kus isikuandmed võivad sattuda ükskõik kelle kätte. Sellise võimalusega peab andmesubjekt arvestama, kui ta avalikustab *Facebookis* isikuandmeid. Samuti peaks selline teave olema rohkem esile toodud.
Euroopa Liidu kodanikud on sõlminud küll kokkuleppe *Facebook Ireland Ltd*-ga, mis sätestab, et *Facebook* peab vastavuses olema Euroopa Liidu privaatsussätetega, kuid kasutajad on samuti

[49] *Ibid.*
[50] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 8.
[51] J. Mišek (viide 14).
[52] Facebook. Statement of Rights and Responsibilities 31.01.2018. Kättesaadav arvutivõrgus: https://www.facebook.com/legal/terms/update.

oma nõusoleku andnud sellele, et nende isikuandmed edastatakse töötlemiseks Ameerika Ühendriikidesse (seda on aastaid tehtud *Safe Harbour* kokkuleppe alusel).[53] Seega on vajalik lugeda kasutustingimusi ja muid olulisi dokumente, et teada, kuhu isikuandmed võivad lõpuks sattuda. *Safe Harbour* kokkulepe on nüüdseks tühistatud ja asendatud *Privacy Shield* kokkuleppega, kuid ka selle kokkuleppe puhul on kahtlusi, kas see tagab piisavalt kõrge andmesubjektide isikuandmete kaitsetaseme.[54] Siiani olnud olukordi, kus andmesubjektid ei ole lugenud vajalikku informatsiooni või ei ole sellesse süvenenud. Seda olukorda võib parandada üldmääruse aktiivse nõusoleku andmise nõue.

Üldmäärus loetleb põhjenduspunktis 43, millal ei ole nõusolek antud vabatahtlikult: kui on tegemist avaliku sektori ja andmesubjekti vahelise suhtega; kui ei ole võimalik anda erinevatele isikuandmete töötlemise toimingutele eraldi nõusolekut ja kui lepingu täitmine on pandud sellisest nõusolekust sõltuma, kuigi see pole lepingu täitmiseks vajalik.[55] Juhis nõusoleku rakendamiseks esitab näite: mööblipood võtab ostjatelt nõusoleku ning jagab ostja isikuandmeid teiste mööblipoodidega, kuid see pole tegelikkuses vajalik teenuse osutamiseks. Seega üldmääruse mõttes selline nõusolek ei kehti. Samal ajal on võimalik, et nõusolek kehtib, kui on konkreetselt kirjas, millistele kolmandatele osapooltele teave edastatakse ning ostjal on võimalik anda aktiivne nõusolek sellele eesmärgile.[56] Kindlasti on paljudel ettevõtetel olnud vajadust analüüsida, mis probleemid võivad seoses nõusolekuga neid ees oodata ning muuta ankeete/küsimustikke vastavalt üldmäärusele (eriti seoses isikuandmete edastamisega koostööpartneritele). Vabatahtlikkuse põhimõtte sisustamine ja rakendamine võib mitmete isikuandmete töötlemise puhul tuua ettevõtetele kaasa probleeme, sest see ei pruugi täiesti arusaadav alati olla. Samal ajal tagab see nõue suuremal määral andmesubjektide informatsioonilist enesemääramisõigust, kuid loob riive ettevõtja huvidele. See tekitab ebakindlust selles osas, kas nõusolek on alati vabatahtlikult antud ning kehtiv või mitte. Autor on arvamusel, et riive ettevõtjate huvidele on olemas. Eelkõige peavad ettevõtted üldmääruse kohaldamise alguses tegema mitmeid analüüse isikuandmete töötlemise osas, kuid hiljem peaks halduskoormus vähenema.

Nõusolek on kahtlemata oluline, kuid vabatahtlikkuse osas tekib küsimus, kui paljud andmesubjektid suudavad teadlikku ja läbimõeldud nõusolekut anda. Teine küsimus on selles,

[53] S. Kulevska. Humanizing the Digital Age: A Right to Be Forgotten Online? – Faculty of Law. Lund University 2014.
[54] B. Marr. Privacy Shield - Is Safe Harbour's Replacement Up To The Job In 2017? – Forbes 29.03.2017.
[55] Euroopa Parlamendi ja Nõukogu määrus 2016/679.
[56] Information Commissioner's office. Consultation: GDPR consent guidance 2017.

kuidas sellist informeeritud nõusolekut mõjutab digitaalse maailma keskkond, mida iseloomustab kiirus. Nendele küsimustele pole täpset vastust võimalik anda, kuid on tõenäoline, et paljud andmesubjektid ei ole teadlikud nende nõusolekuga seotud tagajärgedest. Eelkõige ei ole nõusolek tihti teadlik, läbimõeldud samm, sest esitatud teavet ei loeta ega mõisteta.[57] Üldmäärus on üritanud seda olukorda parandada sellega, et inimesed peavad andma aktiivse nõusoleku isikuandmete töötlemiseks ehk peaksid rohkem tähelepanu pöörama andmete töötlemise tingimustele. Samuti peaks see suuremal määral tagama informatsioonilise enesemääramisõiguse teostamist, sest mõeldakse rohkem läbi, millist infot soovitakse avaldada. Samas ei ole välistatud võimalus, et andmesubjektidele tekib riive informatsioonilise enesemääramise osas, sest ei süveneta töötlemise eesmärkidesse või on need eesmärgid ebamäärased/keerulised. Samal ajal peab ka andmesubjektile endale jääma vastutus oma isikuandmete jagamise eest.

Üldmääruse üheks oluliseks printsiibiks on see, et isik peab andma nõusoleku nö aktiivse tegevusega, mitte passiivsega.[58] Peab olema täiesti arusaadav, millele on isik oma nõusoleku andnud – selle jaoks on vajalik andmesubjekti poolt antud selge ja arusaadav signaal. See võib hõlmata veebisaidi külastamisel nö kasti märkimist, infoühiskonna teenuste tehniliste sätete valimist või muud avaldust või käitumist, mis selgesõnaliselt näitab selles kontekstis, et andmesubjekt nõustub oma isikuandmete kavandatava töötlemisega. Selline tegevus tähendab, et andmesubjektil peab olema võimalus valida. Näiteks võivad positiivsed aktiivse nõusoleku meetodid sisaldada nõusolekut avalduse vormis, suulise kinnitusena, allkirja vormis või tehniliste sätete vahetamise kaudu. Põhimõte on see, et nõusolek peab olema antud subjekti poolt teatud tegevust nõudva toiminguga. Lubatud ei ole tugineda vaikimisele, tegevusetusele, vaikeseadistustele, eelvalikukastidele või üldtingimustele.[59] Eelpool mainitud viis tagab nõusoleku ühemõttelisuse. Oluline on märkida, et tehnoloogia areng võib tuua uusi viise andmesubjektide teavitamiseks, mis võivad autori hinnangul olla efektiivsemad tavalistest kirjalikest vormidest ning tagada suuremal määral andmesubjekti informatsioonilist enesemääramist: näiteks andmesubjektide aktiivset tegevust nõudvad videod, häälsõnumid.

Nõusolekut saab küsida kirjaliku või salvestatud suulise avalduse kaudu. Kirjalikku taasesitamist võimaldav vorm on ilmselt kõige otstarbekam viis tagada nõuetele vastavus. See võib toimida nii, et andmesubjekt kirjutab andmetöötlejale e-kirja, milles selgitab, millega ta

[57] P. Blume (viide 46).
[58] S. Montelone (viide 13).
[59] Information Commissioner's office. Consultation: GDPR consent guidance 2017.

täpselt nõustub.[60] Kirjalikus ja suulises vormis võib nõusolek esineda järgmistes formaatides: võib olla vabas vormis kirjalik vorm ilma täisnimeta; kirjalikku taasesitamist võimaldav vorm, milleks võib olla täisnimega e-kiri; digiallkirjaga elektrooniline vorm; omakäelise allkirjaga lihtkirjalik vorm või salvestatud suulise vormi korral näiteks vabas vormis suuline avaldus ilma täisnimeta, täisnimega helisalvestis. Samas ei ole e-kirja teel nõusoleku saatmine realistlik ega praktiline. Sellisel viisil nõusoleku andmine nõuab ressurssi ja aega nii ettevõtte kui ka andmesubjekti enda poolt. See on ebamõistlik viis arvestades ettevõtte huve võimalikult kiiresti ja efektiivselt äri ajada. Kõige lihtsam oleks tagada nõusoleku andmine nö valikukasti märkimisega.

Probleemiks on kindlasti ka see, et sageli on andmesubjektidel vähe valikuid: kui soovitakse teenust kasutada, peab ka tingimustele vastama - kui andmesubjekt ei märgi nõusoleku kasti linnukest, siis juurdepääs teenusele lükatakse tagasi. Pole ka häid alternatiive: enamik teenusepakkujaid soovivad kohaldada samu tavasid ja sarnaseid andmetöötlustingimusi ning enamkasutatavate teenuste puhul, näiteks *Facebook, Google* või *Twitter*, ei ole reaalset valikut enamikel inimestel. Praktikas pole alternatiivseid ärimudeleid, mis tooksid tulu teistest allikatest. Seetõttu koostatakse kasutajaandmetest profiile ja kasutatakse neid isikuandmeid reklaami edastamiseks. Kuigi tasulised teenused on teoreetiliselt võimalikud, ei ole liikumine tasuta teenustelt tasulistele teenustele midagi, mida enamik internetikasutajatest sooviks teha.[61] Autori hinnangul ei pruugi üldmäärus lahendada probleemi, et enamik internetikasutajatest siiski peab liialt palju isikuandmeid andma teenuseosutajale, kuid loodetavasti hakkavad ettevõtted lähtuma suuremal määral andmete minimaalsuse (isikuandmeid töödeldakse nii vähe kui võimalik)/eesmärgikohasuse põhimõtetest.

Nõusoleku vabatahtlikkuse ja ühemõttelisuse aspektid on üldmääruse kohaselt väga olulised. Seda ka seetõttu, et direktiivi alusel oli kohati keeruline andmesubjekti nõusolekut hinnata, kuna direktiivi puhul oli liikmesriikidel rohkem vabadust ning nõuded nõusolekule võisid liikmesriigiti mingil määral erineda. Samas on keeruline mõista, milline täpselt peab nõusolekuvorm olema (sisuline ning formaalne vorm), et see vastaks üldmääruse nõuetele. See on jäänud hetkel mitmeti tõlgendatavaks ning antud juhul võib see oleneda ka siseriiklikest aktidest. Samuti võivad eesmärgid muutuda või on neid keeruline sõnastada. Autor nõustub kindlasti üldmääruse ideega praegust olukorda parandada, sest paljudes erinevates

[60] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 16.
[61] B. Koops (viide 45).

nõusolekuankeetides on kohati keerulise sõnastusega tekst või puudulik info ning inimese eest on märge juba nö kastikesse tehtud. See pole taganud tegelikku tulemust, mis peaks isikuid reaalselt teavitama nende õigustest ja viisidest, kuidas nende andmeid töödeldakse. Selline passiivse nõusoleku lahendus tagab ainult inimese poolt automaatse kinnituse ilma mõtlemata, millele see kinnitus täpsemalt anti. Samas on üldmäärus tekitanud ebakindlust nõusolekule kohalduvate nõuete osas, sest arvesse peab võtma mitmed tegureid, mis on kohati mitmeti tõlgendatavad. Seega võib öelda, et üldmäärus pole nõusolekule kohaldatavate nõuete rakendamise osas piisavalt õigusselge ning vajalik on siseriiklikult teatud aspekte täpsustada (supra 1.1.3.).

1.2.3. Eesmärgikohasuse põhimõte

Euroopa Komisjon on korraldanud uuringu välja selgitamaks internetikasutajate arvamusi isikuandmete kohta. Enamik Euroopa internetikasutajatest väitis, et nad olid kas alati või mõnikord informeeritud isikuandmete tingimustest ja edasistest kasutusviisidest, kuid ligikaudu kolm viiendikku ütlesid, et neid ei ole kunagi teavitatud sellest või seda on tehtud harvadel juhtudel.[62] See uuring näitab, et olukorda peab kindlasti informeerituse osas parandama. Seetõttu on üldmäärus eesmärgikohasuse põhimõtte olulisust rõhutanud ja karmistanud siiani kehtinud reegleid. Ka Riigikohus on rõhutanud, et isikuandmete töötlemine/avaldamine peab olema kooskõlas andmetöötluse eesmärgikohasuse põhimõttega.[63] Seega võib öelda, et eesmärgikohasus on üks olulisemaid nõudeid, mis on üldmääruses nõusolekule kehtestatud.

Isikuandmete kaitse üldmäärus sätestab põhjenduspunktis 39, et eesmärgid isikuandmete töötlemiseks peaksid alati olema õiguspärased, selged ja konkreetsed ning need tuleks kindlasti määrata kindlaks andmete kogumise ajal. Isikuandmed peaksid olema asjakohased ning olema sisult sellised, mis on töötlemiseks reaalselt vajalikud. Samuti ütleb üldmääruse artikkel 5 lõige 1 punkt b, et isikuandmeid peab töötlema kindlaksmääratud ja õiguspärastel eesmärkidel (nö „eesmärgi piirang“).[64] Kooskõlas eesmärgikohasuse põhimõttega ning üldmääruse põhjenduspunktiga 32 võib nõusolek hõlmata erinevaid toiminguid, kui nendel toimingutel on samad eesmärgid. Oluline on see, et konkreetne nõusolek saab olla vaid siis, kui andmesubjekte

[62] European Commission. Attitudes on Data Protection and Electronic Identity in the European Union. – Special Eurobarometer 359 2011. Kättesaadav arvutivõrgus: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf.
[63] RKTKo 3-2-1-159-14 p 14.
[64] Euroopa Parlamendi ja Nõukogu määrus 2016/679.

teavitatakse täpselt nende isikuandmete kasutamisega seotud eesmärkidest. Kui vastutav töötleja töötleb isikuandmeid nõusoleku alusel ja soovib andmeid töödelda uue eesmärgi saavutamiseks, peab vastutav töötleja taotlema andmesubjektilt uut nõusolekut uue töötlemise eesmärgil.[65]

Eesmärgikohasuse põhimõtte kohta selgitab Andmekaitse Töörühm, et konkreetne eesmärk peab olema piisavalt üksikasjalik, et andmesubjektil oleks võimalik kindlaks teha, milleks töödeldakse tema andmeid. Töörühm märgib, et andmetöötlejad peaksid vältima ebamääraseid või liiga üldisi eesmärke. Sellised eesmärgid nagu „kasutajakogemuse parandamine", „turustus", „IT-turvalisus" ja „tulevased teadusuuringud" ei ole piisavalt täpsed. Täpsusaste, millele nõusoleku küsimusvorm peaks vastama, sõltub konkreetsest kontekstist ja asjassepuutuvate isikuandmete tüübist, mille jaoks andmeid kogutakse. Mõnel juhul võib eesmärkide sõnastamiseks sobida lihtsam ja üldisem keel, teistel juhtudel võib olla vaja üksikasjalikumat teavet.[66] Eesmärgikohasus ja selgus on kindlasti olulised printsiibid, arvestades ka näiteks etteheiteid ühele suurimale meediagigandile *Google'le*, mille puhul on välja toodud, et nende andmetöötlustegevus on väga keerukas ja nad töötlevad paljusid andmeid, mida neil tegelikult enda teenusepakkumise jaoks vaja ei lähe. Samas on paljudele isikutele nii eraelus kui ka tööl vajalikud *Google-ga* seotud teenused.[67]

Esile võib tuua ka nö nutikate linnade (ingl. k. - *smart city*) andmekaitsealaseid probleeme, kus kasutatakse eri liike andmekogumisseadmeid (nt videokaamerad), et vajadusel kiiresti erisugustele olukordadele reageerida. Lahendused, milleks on sh ka nõusolekuankeedid ja teavitused, ei ole piisavalt tõhusad, sest inimestel puudub motivatsioon ja aeg, et neid lugeda ja nendest aru saada. Siin võiks kasutusele võtta tehnilisi lahendusi, kuid erinevate meetmete puhul on oluline läbi viia uuringuid välja selgitamaks, millised nõusoleku andmise viisid oleksid kõige efektiivsemad. Samuti peaks muutma rangemaks nõusoleku alusel andmete töötlemise ning seda ka teatud juhtudel keelama.[68] Üldmääruse kohaselt ei lubata andmetöötlust sellisel juhul, kui andmesubjekt on kasutustingimustega küll nõustunud, aga töödeldakse infot, mis pole vajalik teenuse osutamiseks. Mitmeid olulisi küsimusi on selle kohta, kuidas ettevõtted

[65] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 11.
[66] Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. – European Commission, 02.04.2013, page 16.
[67] J. Rauhofer. Of Men and Mice: Should the EU Data Protection Authorities Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle? – European Data Protection Law Review 2015.
[68] L. Edwards. Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. – European Data Protection Law Review 2016.

saavad kehtivaid nõusolekuid ja millistel juhtudel on võimalik õigustatud huvi töötlemise aluseks võtta.[69]

Vastutavatel andmetöötlejatel on kohustus esitada konkreetne teave iga nõusoleku taotluse kohta. Seega on andmesubjektidel võimalik anda konkreetne nõusolek igale eesmärgile. See küsimus kattub nõudega, et vastutavad töötlejad peavad esitama selge teabe. Kehtiva nõusoleku saamiseks on vaja vähemalt järgmist teavet: 1) vastutava töötleja andmed; 2) kõigi töötlemistoimingute eesmärgid, milleks nõutakse nõusolekut; 3) milliseid (liiki) andmeid kogutakse ja kasutatakse; 4) nõusoleku tagasivõtmise õiguse olemasolu; 5) teavet üksnes automatiseeritud töötlemisel põhinevate otsuste kohta; 6) info, kui nõusolek on seotud andmete kolmandatesse riikidesse edastamisega.[70] See on kindlasti andmesubjekti seisukohalt suur edasiminek läbipaistvuse osas, sest siiani pole andmesubjekte nii põhjalikult isikuandmete kasutamise ja eesmärkide osas informeeritud. Näitena võib tuua, et paki tellimisel pakiautomaati küsitakse andmesubjekti aadressi, kuid eesmärki, miks sellist infot vaja on, andmesubjektile ei esitata. Kui isik pakile järele ei lähe, siis see tagastatakse üldjuhul saatjale või hoiustatakse postkontoris. Seega ei saa teatud juhtudel väita, et juhul, kui isik ei tule pakiautomaati pakile järele, siis saadetakse see andmesubjektile koju. Vähemalt võiks andmesubjektile jätta vabaduse valida, kas ta soovib aadressi lisada või mitte.

Siiani on probleemiks olnud see, et andmetöötlejad lisavad informatsiooni andmete töötlemise kohta üldtingimustesse või privaatsuspoliitikasse, aga neist ei ole alati lihtne aru saada, sest need on keeruliselt sõnastatud.[71] Isikuandmete üldmääruse alusel peab eesmärgi muutudes küsima nõusolekut uuesti, v.a siis, kui eesmärk on kooskõlas algse eesmärgiga.[72] Peab ka lisama, et hetkel väljatöötatud siseriiklik nõusoleku kontrollnimekiri[73] on asjalik ja abistav, kuid täpsustub osade punktide osas, kui tulevad konkreetsemad suunised.

Eesmärgikohasuse põhimõte võib olla ettevõtete jaoks problemaatiline, sest nõuab teenusepakkujatelt ressurssi ja pidevat eesmärkide analüüsimist. Üldmääruse mõte on samal ajal oluline ja vajalik selleks, et oleks tagatud andmesubjekti informatsiooniline enesemääramine ning teadlikkus isikuandmete töötlemise eesmärkide kohta. Tähtis on ka

[69] A. A. I. Vranaki. Regulating Social Networking Sites: Facebook, Online Behavioral Advertising, Data Protection Laws and Power. – Rutgers Computer & Technology Law Journal 2017.
[70] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 13.
[71] H. Ursic. Legal Barriers and Enablers to Big Data Reuse. – European Data Protection Law Review 2016.
[72] A. Bussche Freiherr, A. Zeiter. Implementing the EU General Data Protection Regulation: A Business Perspective. – European Data Protection Law Review 2016.
[73] Andmekaitse Inspektsioon. Nõusoleku kontrollnimekiri 26.06.2017. Kättesaadav arvutivõrgus: http://www.aki.ee/et/andmekaitse-reform/nousoleku-kontrollnimekiri.

küsimus, et kas nõusoleku alusel peaks võimalikult vähe isikuandmeid töötlema ehk isikuandmete töötlemise lubatavus peaks tulenema pigem teistest seaduslikest alustest (seadus, lepingu täitmine, õigustatud huvi jne), sest see tagab olukorra, kus ei küsita andmesubjektidelt ülemäära palju isikuandmeid ning võimaldab isikutel end suuremal määral informatsiooniliselt määrata. Sellisel juhul ei peaks andmesubjektid edastama andmeid, mida nad annavad eelkõige seetõttu, et oleks võimalik teenust kasutada. Autor on seisukohal, et nõusoleku alusel peaks töötlema võimalikult vähe isikuandmeid ning pigem oleks vajalik leida teisi seaduslikke aluseid isikuandmete töötlemiseks. Nõusolekuankeetide puhul (eriti veebitaotluste osas) jääb alatiseks alles oht, et tekib riive andmesubjektide informatsioonilisele enesemääramisele, sest andmesubjektid ei süvene piisavalt sellesse, mis on ankeedis kirjas või ei saa sellest aru ning enese teadmata võivad andmed olla sattunud näiteks kolmandate isikute valdusesse. Ettevõtjad ei peaks sellisel juhul liialt analüüsima erinevaid nõusolekule kohaldatavaid nõudeid ning nõusoleku kehtivust. Samal ajal võib tekkida riive ettevõtja huvidele, sest ettevõtjad on huvitatud võimalikult paljudest klientidest ning nende jaoks on isikuandmed oluliseks vahendiks müügitöö tegemisel. Seega tuleks kindlasti rõhutada ka andmesubjekti enda vastutust informatsioonilise enesemääramisõiguse sisustamisel.

1.2.4. Nõusoleku tagasivõtmine

Nõusoleku tagasivõtmine on samuti oluline põhimõte üldmääruses. Eesti isikuandmete kaitse seaduses on märgitud, et andmesubjektil on õigus nõusolek tagasi võtta (supra 1.1.3.). Näiteks Soome ja Norra vastav seadusandlus ei ole ette näinud andmesubjektile õigust juba antud nõusolekut igal ajal tagasi võtta, kuid Rootsi isikuandmete kaitse seadus sarnaselt Eesti isikuandmete kaitse seadusega võimaldab andmesubjektil juba antud nõusolek tagasi võtta. Eesti IKS-is sisalduv andmesubjekti õigus nõusolek igal ajal tagasi võtta on õiguslikus mõttes pigem erandlik olnud.[74] Riigikohus on lahendis nr 3-2-1-153-16 leidnud, et nõusoleku tõendamise kohustus on isikuandmete töötlejal ja isikul on igal ajal võimalik nõusolek tagasi võtta.[75] Riigikohtu otsus kinnitab isikuandmete kaitse seaduses sätestatud põhimõtet.

Üldmäärus sätestab artiklis 7 lõikes 3, et andmesubjektil on õigus oma nõusolek igal ajal tagasi võtta ja nõusoleku tagasivõtmine ei mõjuta enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust. Andmesubjekti teavitatakse sellest enne nõusoleku andmist. Nõusoleku tagasivõtmine on sama lihtne kui selle andmine.[76] Huvitava näitena võib välja tuua

[74] M. Männiko, lk 102.
[75] RKTKo 3-2-1-153-16 p 23.
[76] Euroopa Parlamendi ja Nõukogu määrus 2016/679.

krediidiasutuse. Andmesubjekt saab krediidiasutuselt laenu ning tingimusena on seatud, et maksehäirete korral on krediidiasutusel õigus avaldada andmesubjekti andmed võlglaste nimekirjas. Andmesubjekt nõustub sellega ning mingi aja pärast tekivad maksehäired, kuid andmesubjekt saab kasutada oma õigust nõusolek tagasi võtta ning keelata isikuandmete avaldamine. Siinkohal pannakse andmetöötleja pannakse olukorda, kus andmesubjekti tahteavaldus ei too kaasa õiguspärast ootust ka selle püsimajäämisele.[77] Nõustun kindlasti viimase väitega, sest nõusoleku tagasivõtmine võib tekitada õiguslikus mõttes mitmeid ootamatuid olukordi. Kuna nõusolekut on võimalik tagasi võtta, siis see loob ettevõtetele ebakindlust isikuandmete töötlemise osas. Samal ajal peab arvesse võtma, et andmesubjekti õiguste rakendamisel tagab selline õigus suuremal määral informatsioonilist enesemääramist. Isikul on võimalik nõusolek tagasi võtta ning konkreetseid isikuandmeid ei tohi enam edasi töödelda, kui teist alust selle jaoks ei ole. Eestis on isikuandmete kaitse seaduses antud põhimõte ka juba varasemalt kehtinud, kuid peale uue üldmääruse kohaldamist on andmesubjektid selle õigusega rohkem kursis ning on täiesti võimalik, et nõusoleku tagasivõtmist hakatakse rakendama kordades rohkem.

Andmekaitse Töörühm on selgitanud, et üldmäärus ei sätesta, et nõusoleku andmine ja tagasivõtmine peab alati toimuma sama tegevuse kaudu. Samas on lisatud, et kui nõusolek saadakse elektroonilisel teel ainult ühe hiireklõpsu, viipamise või klahvivajutuse abil, peavad andmesubjektid suutma praktikas seda nõusolekut sama hõlpsasti ka tagasi võtta. Kui nõusolek saadakse spetsiifilise kasutajaliidese (näiteks veebisait, rakendus, sisselogimiskonto või e-post) kaudu, siis peab olema võimalik nõusolek tagasi võtta sama elektroonilise liidese kaudu, kuna teisele liidesele üleminek ainult nõusoleku tagasivõtmise tõttu nõuab põhjendamatuid jõupingutusi. Lisaks peab vastutav töötleja võimaldama nõusoleku tagasivõtmise tasuta või teenusetaset alandamata.[78]

Nõusoleku tagasivõtmise puhul peab andmetöötleja lõpetama andmete töötlemise (kui ei ole muud seaduslikku alust selleks) ning andmed kustutama või anonümiseerima. Andmetöötlejad peaksid seetõttu algusest peale selgeks tegema, millist eesmärki kohaldatakse iga andmehulga suhtes ja millistele seaduslikele alustele tuginetakse. Juhul, kui andmesubjekt loobub oma nõusolekust ja vastutav töötleja soovib jätkata isikuandmete töötlemist mõnel muul seaduslikul alusel, ei saa nad nõusolekust (mis on tagasi võetud) vaikimisi üle minna teisele seaduslikule alusele, vaid andmesubjekti peab sellest teavitama.[79] Teavitamiskohustus on väga oluline

[77] M. Männiko, lk 103, 104.
[78] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 21.
[79] *Ibid*, page 22.

põhimõte, mis kaasneb mitmete andmekaitsega seotud tegevustega. Samuti annab see andmesubjektile info, miks tema isikuandmeid siiski edasi töödeldakse.

Üldmäärusele on etteheidetud, et pole täpsustatud, kuidas peaks praktikas käima nõusoleku tagasivõtmise menetlus. Samas on võimalik aru saada, et see protsess peab olema sama lihtne kui nõusoleku andmine.[80] Tulevikus võib olla mitmeid arusaamatusi ka nõusoleku tagasivõtmisega. Nõusoleku tagasivõtmine on tehniliselt keeruline, sest paljud isikuandmed on mitmetes erinevates infosüsteemides ja dokumentides. Vajalik on tagada olukord, kus isikuandmeid ei oleks enam üheski süsteemis ega dokumendis, seega peab IT-alaselt tagasivõtmise menetlust analüüsima. Sama kehtib ka isikuandmete kustutamise kohta.

Ameerika Ühendriikide terviseandmete ekspert Stacey Tovino on võrrelnud üldmäärust ja Ameerika Ühendriikide 1996. aasta tervisekindlustuse ülekantavuse ja vastutuse seadust. Õigusaktide sarnasuseks on, et mõlemas on kirjas põhimõte, mille alusel peab nõusoleku tagasivõtmise õigusest andmesubjekti teavitama. Samas on suureks erinevuseks see, et kui üldmäärus sätestab, et nõusoleku tagasivõtmine peab olema võimalikult lihtne, siis tervisekindlustuse ülekantavuse ja vastutuse seadus seda põhimõtet ei kehtesta. Näiteks nõuavad osad haiglad (sh Lõuna-Nevada ülikooli meditsiinikeskus), et nõusoleku tagasivõtmine oleks saadetud tavapärase posti teel või peavad isikud tulema haigla ametniku juurde, kuigi enamjaolt antakse nõusolek veebiteenuste kaudu. Seega on andmesubjektidel keerulisem oma nõusolekut tagasi võtta, mis kindlasti ei ole proportsionaalne võte andmekaitse seisukohalt.[81] Kuna nõusoleku tagasivõtmine on oluline võimalus andmesubjekti jaoks, siis peaks see olema võimalikult lihtne ning täielikult samaväärne nõusoleku andmise võimalusega. Vastasel juhul ei tagata andmesubjektidele võrdseid lahendusi ning neil on palju keerulisem oma õigust tagasivõtmise osas teostada. Seetõttu pean oluliseks üldmääruse põhimõtet, et nõusoleku tagasivõtmine peab olema sama lihtne kui selle andmine.

1.3. Andmesubjekti nõusoleku tõendamiskohustus

1.3.1. Nõusoleku tõendamine üldmääruse alusel

Üldmääruse artikkel 7 lg 1 sätestab, et kui isikuandmete töötlemine põhineb nõusolekul, peab vastutaval töötlejal olema võimalik tõendada, et andmesubjekt on nõustunud oma isikuandmete töötlemisega.[82] Samuti peab kehtiv nõusolek vastama olulistele põhimõtetele (osad printsiibid

[80] D.W. Schartum (viide 18).
[81] S. A.Tovino. The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons. – Seton Hall Law Review 2017.
[82] Euroopa Parlamendi ja Nõukogu määrus 2016/679.

analüüsitud supra 1.2.). Hetkel kehtiv IKS § 12 lg 8 näeb ette, et vaidluse korral eeldatakse, et andmesubjekt ei ole oma nõusolekut andnud ning tõendamise kohustus on isikuandmete töötlejal.[83] Seega pole Eesti puhul nii suure muutusega tegemist, kuid samas on nõuded muutunud konkreetsemaks nõusoleku kehtivuse osas ja paljudel ettevõtetel pole varasemalt kogutud nõusolekud vastavuses uue isikuandmete kaitse üldmäärusega. Järgnevalt analüüsin kitsaskohti seoses nõusoleku olemasolu tõendamisega.

1.3.2. Nõusoleku tõendamine suulises vormis

Võib öelda, et Eestis on siiani populaarne telefonimüük, mille kaudu üritatakse müüa kas ajalehti või muid tooteid. IKS § 12 lg 5 näeb ette, et andmesubjektil on õigus igal ajal keelata teda käsitlevate andmete töötlemine tarbijaharjumuste uurimiseks või otseturustuseks ja andmete üleandmiseks kolmandatele isikutele, kes soovivad neid kasutada tarbijaharjumuste uurimiseks või otseturustuseks. IKS § 4 kohaselt on biomeetrilised andmed delikaatsed isikuandmed.[84] IKS § 4 lg 2 p 5 nimetab biomeetriliste andmetena eelkõige sõrmejälje-, peopesajälje- ja silmaiirisekujutist ning geeniandmeid. Biomeetrilised andmed on mitmesugused bioloogilised, füüsilised, psühholoogilised, käitumuslikud või sarnased omadused, mida kasutatakse isiku tuvastamisel. Näiteks kasutatakse tuvastamisel lisaks eelpool nimetatutele ka silma võrkkesta, näojooni, kõrva kuju, kehalõhnu, häält, peopesa geomeetriat.[85] Seega kuulub isiku hääl biomeetriliste andmete hulka, mis on delikaatsed isikuandmed ning seega tugevama kaitse all. Üldmääruse artikkel 4 punkt 14 alusel on biomeetrilised andmed konkreetse tehnilise töötlemise abil saadavad isikuandmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist. Üldmääruse artikkel 9 lõike 1 järgi on biomeetrilised isikuandmed eri liiki isikuandmed, kui neid andmeid kasutatakse füüsilise isiku kordumatuks tuvastamiseks.[86] Kui kõne salvestatakse ning seda on vajalik nõusoleku tõendamiseks, siis peavad need andmed olema seotud konkreetse füüsilise isikuga.

Üheks aspektis kõnede salvestamise puhul on ka see, et ettevõttel on vajalik saada nõusolek kõne salvestamiseks. Eraettevõttes saab kõnesid salvestada kas nõusoleku või kliendiga sõlmitud lepingu alusel. Sellest tulenevalt peab kõne teist poolt lindistamisest hiljemalt kõne alguses selgelt teavitama ning salvestamiseks peab olema isiku nõusolek. Nõusoleku andmine

[83] Isikuandmete kaitse seadus. – RT I, 06.01.2016, 10.
[84] *Ibid.*
[85] Andmekaitse Inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal 2014.
[86] Euroopa Parlamendi ja Nõukogu määrus 2016/679.

peab olema inimese vaba ja informeeritud tahteavaldus.[87] Kui soovitakse saada andmesubjekti nõusolekut näiteks kontaktandmete töötlemiseks, siis on oluline, et oleks olemas nõusolek või muu õiguslik alus kõne salvestamiseks.

Huvitav on ka küsimus, et kui telefoni teel toimub kõne salvestamine, kas sellisel juhul peaks isik täislausena ütlema, et ta on nõus enda isikuandmete töötlemisega ning kõne salvestamisega või piisab sellest, kui isik ütleb, et ta on nõus. Lahenduseks võib ka see olla, kui töötatakse välja süsteem, kus telefonikõne salvestamisel öeldakse, et juhul, kui te ei soovi anda nõusolekut kõne salvestamiseks, siis katkestage kõne. Juhul, kui soovite anda nõusoleku sellise tegevuse jaoks, siis oleks vajalik kinnituseks vajutada kindlat numbrit. Sellise süsteemi abil oleks võimalik tõestada, et andmesubjektil oli võimalus keelduda isikuandmete töötlemisest. Ilmselt peaksid juhised sisaldama põhjendusi, miks antud toiming on vajalik – et andmetöötlejal oleks olemas kehtiv ning aktiivne nõusolek isikuandmete töötlemiseks. Võib ka tekkida selline olukord, et helistatakse isikule (telefoninumber on saadud avalikest andmebaasidest) ning saadakse telefoni teel andmesubjektilt kontaktandmed. Samuti küsitakse isikult nõusolekut nende andmete töötlemiseks. Selleks, et nõusolek oleks kehtiv, peaksid olema suuliselt öeldud andmetöötluse eesmärgid, õiguslik alus ja muu vajalik info. Kui näiteks andmetöötleja saadab andmesubjektilt saadud e-mailile pakkumisi või taotluse ning teeb seda nõusoleku alusel, siis oleks ikkagi vaja telefoni teel täpselt selgitada, miks on e-maili aadress vajalik ning mis on eesmärk selle info töötlemisel. Problemaatiline on ka telefonikõnede salvestiste mahukus ning ajaline säilitamine, sest peab lähtuma andmete minimaalsusest ja vajalikkusest (tõendamise mõttes). Kui andmesubjekt väidab, et tema pole isikuandmete töötlemiseks nõusolekut andnud, siis peab vastutav andmetöötleja vastupidist tõendama hakkama.

Euroopa Liidus hakkab kohalduma e-privaatsuse määrus, mis täpsustab otseturustuse põhimõtteid ning muudab kontrollitumaks telefoni teel pakkumiste korraldamise. E-privaatsuse määruse põhjenduspunkt 35 sätestab, et telefoni teel otseturustuse eesmärgil helistamise puhul peab olema andmesubjektile nähtav telefoninumber või peab olemas olema spetsiaalne eesliide.[88] Samuti tõhustatakse telefoninumbrite blokeerimise võimalusi. Üldmääruse artikkel 21 lg 3 sätestab, et kui andmesubjekt esitab vastuväiteid otseturustuse eesmärgil toimuva andmete töötlemise suhtes, siis ei tohi isikuandmeid sellisel eesmärgil enam töödelda.[89]

[87] Andmekaitse Inspektsioon. Telefonikõnede salvestamise lubatavuse juhend 2012.
[88] Euroopa Parlamendi ja Nõukogu määrus, 10.01.2017, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). Kättesaadav arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52017PC0010.
[89] Euroopa Parlamendi ja Nõukogu määrus 2016/679.

Enamikel juhtudel jäävad andmetöötlejad isikuandmeid töötlema ilmselt õigustatud huvi alusel, mitte nõusoleku alusel, sest üldmääruse põhjenduspunkt 47 sätestab, et selle alusel on võimalik otseturustuses andmeid töödelda.[90] Samas on oluline rõhutada, et teatud valdkondades on selline tegevus lubatud ainult nõusoleku alusel (näiteks krediidiasutuste puhul) ning andmesubjektil on õigus keelduda isikuandmete töötlemisest sellisest eesmärgist lähtudes.

1.3.3. Nõusoleku tõendamine kirjalikel viisidel

Kirjalik viis[91] nõusoleku küsimiseks ei ole üldmääruses sätestatud ainukeseks nõusoleku saamise viisiks. Kirjaliku nõusoleku nõude sätestamine kui ainukeseks viisiks nõusoleku saamiseks ei oleks olnud mõistlik, sest nõusoleku andmine peaks olema sõltumatu tehnoloogiast. Samuti võivad tulevikus veelgi enam levida muud nõusoleku andmise vormid (seoses infotehnoloogia arenguga) ning sellises olukorras võib kirjaliku nõusoleku nõue osutuda takistuseks. Kirjalikul nõusolekul on kaks põhieesmärki: see tagab nõusoleku selguse ja sel on tõenduslik eesmärk. Seepärast on eelistatum nõusoleku olemasolu kirjalikus vormis.[92] Autori arvates tagab samuti nõusoleku kehtimise kõige efektiivsemalt nõusoleku küsimine ja salvestamine kirjalikel viisidel. See annab võimaluse täpselt kirja panna eesmärgid ning muud vajalikud üldmääruses sätestatud nõuded. Tulevikus võib juhtuda, et isik ei lisa lahtrisse linnukest (näiteks unustab) ja ei nõustu andmete töötlemisega. Sellisel juhul oleks ikkagi vajalik andmesubjektilt nõusolek saada. Mingitel juhtudel on võimalik väita, et andmeid töödeldakse lepingu sõlmimise eesmärgil, kuid alati ei pruugi see nii olla. Veebitaotluste puhul oleks vajalik, et taotlust saab ainult sellisel juhul ära saata, kui on lisatud linnuke kohustuslikesse lahtritesse. Samuti ei pea kirjalikel viisidel nõusoleku võtmise aspektide puhul töötlema andmesubjekti biomeetrilisi/eriliigilisi andmeid (hääl) ning sellisel juhul on väiksem riive just isikuandmete liigi osas. Nii ei teki ka andmesubjektil kohustust anda biomeetrilisi isikuandmeid andmetöötlejale töötlemiseks, mis on autori hinnangul tervitatav informatsioonilise enesemääramisõiguse kontekstis.

Kindlasti on oluline luua ettevõttesiseselt ühtne nõusolekute süsteem, kust oleks vajaduse korral võimalik kiiresti leida asjakohane nõusolek. See peaks olema kergesti kättesaadav. Nõusolekuankeetide puhul peab analüüsima, kas kõik küsitavad andmed on eesmärgipärased ja minimaalsed. Samuti peab jälgima, et sõnastus oleks lihtne ja selge. Kohati tundub, et

[90] *Ibid.*
[91] Kirjalik viis: vabas vormis kirjalik vorm ilma täisnimeta; kirjalikku taasesitamist võimaldav vorm, milleks võib olla täisnimega e-kiri; digiallkirjaga elektrooniline vorm; omakäelise allkirjaga lihtkirjalik vorm.
[92] B. Custers, S.van der Hof, B. Schermer, S. Appleby-Arnold, N. Brockdorff (viide 47).

erinevate ankeetide loomine tekitab rohkem bürokraatiat, kuid see on vajalik, et andmesubjektid mõistaksid erinevaid tagajärgi ja isikuandmete kasutust. Näiteks pankadel on vaja mitmeid isikuandmeid küsida rahapesu ja terrorismi tõkestamise nõuete tõttu ehk seaduse alusel, seega peaks konkreetselt läbi mõtlema, milliseid isikuandmeid on vaja küsida just nõusoleku alusel.

Mitmetes artiklites on soovitatud kaheviisilist kinnitamist, kus oleks garanteeritud turvalisem ja arusaadavam nõusolek. Selleks peaks olemas olema tavaline nõusolekuankeet ja lisaks selle lõpetamisele peaksid andmesubjektid saama e-mailile sõnumi oma nõusoleku kinnitamiseks (see saadetakse lingina). See ei nõua andmetöötlejalt liialt palju ressurssi ning on samuti kindel viis, et nõusolek oleks kehtiv ja tõendaks seda, et isikul ei olnud mitte mingeid kahtlusi nõusoleku andmisel.[93] Paljudel ettevõtetel on selline viis olemas, kuid see võiks autori arvates kindlasti laialdasemat kasutust leida.

Üldmääruse artikkel 7 lg 2 käsitleb kirjalikke avaldusi nõusoleku kohta. Kui lepingu alusel nõutakse nõusolekut isikuandmete töötlemiseks, siis peab taotlus olema selgelt eristatav teistest küsimustest, mis on lepingus sätestatud. Kui lepingus on mitmeid aspekte, mis pole selle valdkonnaga seotud, siis tuleks nõusolekut käsitelda selgelt eristatavas vormis või täiesti eraldi dokumendis. See põhimõte kehtib nii paberkujul dokumentide kui ka elektrooniliste kohta.[94] Autor nõustub Andmekaitse Töörühma soovitustega ning lisaks sellele ei soovita sellist lahendust, kus on olemas lahter, et isik nõustub isikuandmete töötlemisega ning lahtri juures olevale tärnikesele peale vajutades avaneb eraldi dokumendina oluline info isikuandmete töötlemise kohta. Pigem peaks selline info olema autori hinnangul lahtri juures ning see tagaks ka paremini selle, et isik reaalselt tutvub infoga ja võtab seda arvesse. Kindlasti võiks oluline teave olla rasvases kirjas.

Huvitav valdkond on elektrooniline otseturustus (v.a telefoni teel tehtud pakkumised). Elektroonilise otseturustuse mõistet seaduses defineeritud ei ole, kuid praktikas käsitletakse otseturustusena nii füüsilistele kui juriidilistele isikutele saadetavaid pakkumisi seoses toote müügi või teenuse osutamisega. Tihti on otseturustuse puhul tegemist kommertsteadaannete saatmisega.[95] Täpsemad nõuded on sätestatud elektroonilise side seaduse §-des 103 ja 103[1].

[93] L. Irwin. How to create GDPR compliant consent forms. – IT Governance Blog 2017.
[94] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 15.
[95] Andmekaitse Inspektsioon. Elektrooniliste kontaktandmete kasutamine otseturustuses 2015. Kättesaadav arvutivõrgus:

Kontaktandmete kasutamine otseturustuseks on lubatud sellisel juhul, kui on olemas kasutaja/kliendi eelnev nõusolek. See peab vastama IKS §-s 12 sätestatud tingimustele (nõusoleku vabatahtlikkus, kirjalik taasesitatav vorm, nõusoleku võib tagasi võtta jne) ning kliendile peab selgitama, millist liiki andmeid on turustuseks vaja ning olemas peab olema teave andmete kasutamise kohta.[96] Otseturustuse puhul on tähtis märkida, et elektroonilise edastamise puhul on e-privaatsuse määruse põhjenduspunktis 35 täpsemalt reguleeritud nõusoleku tagasivõtmine – juriidilised ja füüsilised isikud peavad lisama lingi või kehtiva elektronposti aadressi, mida lõppkasutajad saavad kasutada oma nõusoleku tagasivõtmiseks.[97] Seega on võimalik üsna lihtsal viisil ka nõusolek tagasi võtta, mis tagab suuremal määral isiku võimalust end informatsiooniliselt määrata ning omada kontrolli oma isikuandmete üle.

http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/Elektrooniliste%20kontaktandmete%20kasutamine%20otseturustuseks-uuendatud20.02.2015.pdf.

[96] Elektroonilise side seadus. - RT I, 01.07.2017, 2.

[97] Euroopa Parlamendi ja Nõukogu määrus, 10.01.2017, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). Kättesaadav arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52017PC0010.

2. NÕUSOLEKUGA SEOTUD ÕIGUSLIKUD PROBLEEMID ÜLDMÄÄRUSE JA SENISE KOHTUPRAKTIKA KOHASELT

2.1. Nõusolek andmete ülekandmisel

2.1.1. Andmete ülekandmise õigus

Andmete ülekandmise õigus on üks suuremaid muudatusi, mis üldmäärusega kaasneb. Üldmääruse artikkel 20 lg 1 selgitab uue mõiste olemust: „*Andmesubjektil on õigus saada teda puudutavaid isikuandmeid, mida ta on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul ning õigus edastada need andmed teisele vastutavale töötlejale, ilma et vastutav töötleja, kellele kõnealused isikuandmed on esitatud, seda takistaks, kui a) töötlemine põhineb artikli 6 lõike 1 punktis a või artikli 9 lõike 2 punktis a osutatud nõusolekul või artikli 6 lõike 1 punktis b osutatud lepingul ning b) töödeldakse automatiseeritult*“.[98] Artikkel 6 lõige 1 punkt a sätestab üldise põhimõtte, mis puudutab isiku nõusoleku andmist isikuandmete töötlemiseks ühel või mitmel eesmärgil ning artikli 9 lõikes 2 on sama põhimõtte kirjeldus eriliigiliste isikuandmete osas. Artikkel 20 täpsustab lõigetes 2-3, et andmesubjekt saab nõuda isikuandmete ülekandmist otse teisele andmetöötlejale, kui see on tehniliselt võimalik ning seda õigust ei kohaldata avalikes huvides ülesande täitmiseks.. Tehnilise võimekuse juures on oluline märkida, et andmeid peaks olema võimalik süsteemselt üle kanda. Näiteks loovad kaks sideettevõtet omavahelise süsteemi, mille abil on võimalik lihtsasti andmeid edasi anda.

Uue isikuandmete kaitse seaduse seletuskirjas on välja toodud, et täiesti uue õigusena sätestatakse õigus andmete ülekandmisele ühe töötleja juurest teise juurde, mis füüsiliste isikute jaoks võib lihtsustada näiteks teenusepakkuja vahetust (telekommunikatsiooniteenused, kommunaalteenused jm). Ülekandmise õigus võib kohalduda juhtudel, kus töötlemine põhineb andmesubjekti nõusolekul, lepingu täitmisel või kui andmeid töödeldakse automatiseeritult. Kui see on tehniliselt teostatav ning võimalik, võib andmesubjekt nõuda, et vastutav töötleja edastab andmed otse teisele vastutavale töötlejale. Samuti on lisatud, et muudatusega võib kaasneda halduskoormuse suurenemise erasektori isikuandmete töötlejatele.[99] Uus õigus suurendab kindlasti halduskoormust erasektorile, sest peab analüüsima nõusoleku nõuetele vastavust (kuhu lisada, kuidas rakendada). Andmete ülekandmise õigust pole IKS eelnõus eraldi välja toodud, kuid see pole autori hinnangul ka vajalik. Saksamaa föderaalses andmekaitse seaduses pole samuti andmete ülekandmise õigust eraldi välja toodud.

[98] Euroopa Parlamendi ja Nõukogu määrus 2016/679.
[99] Isikuandmete kaitse seaduse eelnõu seletuskiri. 21.03.2018, lk 53-54.

Andmekaitse Töörühm on selgitanud, et uue andmete ülekandmise õiguse eesmärk on suurendada andmesubjektide mõjuvõimu seoses oma isikuandmetega. See parandab isikuandmete liikuvust, võimalik on andmeid kopeerida või ühest IT-keskkonnast teise üle kanda. Selleks võivad olla nende enda, usaldusväärsete kolmandate isikute või uute vastutavate töötlejate süsteemid. See kujutab endast ka võimalust tasakaalustada andmesubjektide ja vastutavate töötlejate suhteid. Kõnealused andmed tuleks saada *„struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul"*.[100] Asjade interneti (*IoT-Internet of Things*[101]*)* seadmete liideste arengute ebaühtlus tekitab probleeme teabe edastamisel ja vastavalt üldmääruse nõuetele selgesõnalise nõusoleku saamiseks. Asjade interneti seadmete kasutamisel võivad tekkida uued nõusoleku andmise viisid näiteks videote, helisignaalide kaudu või käsitsi viipamise vahendusel. Need uued võtted võivad tekitada vajaduse nõusoleku uueks määratlemiseks ning eemaldumiseks nö traditsioonilistest viisidest (üldtingimused, nõusolekuvormid).[102] Andmekaitse Töörühm on veel näitena esile toonud, et andmesubjekt võib soovida kätte saada oma senise esitusnimekirja või kuulatud lugude ajaloo, et teha kindlaks, mitu korda ta on teatud lugusid kuulanud, millist muusikat ta soovib osta või mõnel muul platvormil kuulata. Samuti võib andmesubjekt tahta kontaktide nimekirja oma veebimeili rakendusest, et koostada näiteks pulmakülaliste nimekiri või saada teavet ostude kohta, mille tegemisel kasutati erinevaid püsikliendikaarte.[103]

Andmesubjektil on küll rohkem võimalusi, aga see eeldab ka nõuetele vastava nõusoleku saamist. Võivad tekkida olukorrad, kus näiteks kantakse üle valeinformatsioon või puudulik info. Selliste olukordade vältimiseks soovitatakse kehtestada kaitsemeetmed tõendamaks, et andmetöötleja tegutseb andmesubjekti nimel. Näiteks on ettevõtetel võimalus sisse seada menetlused, millega tagatakse, et edastatakse sellist liiki isikuandmeid, mida andmesubjekt soovib edastada. Selleks võib hankida andmesubjekti kinnituse kas enne andmete edastamist või veelgi varem.[104]

---

[100] Artikli 29 alusel alustatud Andmekaitse Töörühm. Suunised andmete ülekandmise õiguse kohta, 05.04.2017, lk 3,4.

[101] *Internet of Things* (asjade internet) - Vaatamata *IoT* kasvavale levikule ei ole selle osas ühtses definitsioonis kokkulepitud. *IoT* mõiste alla kuuluvad igapäevaselt kasutatavad tehnoloogilised esemed, mis võimaldavad suhelda füüsilise keskkonna, inimeste ja teistega seadmetega. Arvutid ja mobiilseadmed ei kuulu üldiselt selle alla, kuid nutitelefonid ja tahvelarvutid on osa sellest. – M. Paez, M. L. Marca, The Internet of Things: Emerging Legal Issues for Businesses. – Northern Kentucky Law Review 2016.

[102] L. Urquhart, N. Sailaja, D. McAuley. Realising the right to data portability for the domestic Internet of things. – Pers Ubiquit Comput 2017.

[103] Artikli 29 alusel alustatud Andmekaitse Töörühm. Suunised andmete ülekandmise õiguse kohta, 05.04.2017, lk 5.

[104] Artikli 29 alusel alustatud Andmekaitse Töörühm. Suunised andmete ülekandmise õiguse kohta, 05.04.2017, lk 6.

2.1.2. Kolmandate andmesubjektide isikuandmed andmete ülekandmisel

Võimalikku kahjulikku mõju kolmandate isikute huvidele on püütud parandada artikli 20 lõikes 4 sisalduva klausli lisamisega, et andmete ülekandmine *„ei tohi kahjustada teiste isikute õigusi ja vabadusi“*.[105] Selleks, et kontrollida, kas kolmandate isikute privaatsusõigust kahjustatakse, tuleks rõhutada vastutavate andmetöötlejate ülesannet - leida tasakaal andmesubjekti andmete ülekandmise õiguse teostamise ja teiste õiguste ning vabaduste riive vahel. Kui andmekogusse on kaasatud kolmandate isikute isikuandmed, siis nendel juhtudel tuleb kindlaks teha teine (õigustatud huvi, seadus jne) üldmäärusele vastav töötlemise põhimõte.[106]

Andmekaitse Töörühm on selgitanud, et kui andmekogum sisaldab kolmandate isikute isikuandmeid, tuleb töötlemiseks kindlaks määrata mõni muu õiguslik alus. Näitena on toodud, et vastutav töötleja võib artikli 6 lõike 1 punkti f alusel tugineda õigustatud huvile, eelkõige kui vastutava töötleja eesmärk on pakkuda andmesubjektile teenust, mis võimaldab viimasel töödelda isikuandmeid eranditult isiklikel või kodustel eesmärkidel.[107] See võib hõlmata kasutajaid, kes näiteks analüüsivad energiatarbimist või finantsandmeid, et tekiks parem ülevaade nende tarbimisest. Vastutavad andmetöötlejad peaksid andmesubjektidele pakkuma tehnilisi vahendeid, mis võimaldaksid andmesubjektil jätta alles andmed enda kohta ning välistada kolmanda poole andmed.[108] Tehniliste ja korralduslike meetmete osas peaks üldmäärus julgustama vastutavaid töötlejaid iga andmesubjekti isikuandmeid koguma ja töötlema eraldi, mitte koondatud kujul (nii kaua kui võimalik).[109] Andmekaitse Töörühm on samuti näitena välja toonud, et andmesubjekti pangakonto võib sisaldada isikuandmeid, mis on seotud mitte üksnes kontoomaniku, vaid ka teiste isikute tehingutega (näiteks kui isikud on kontoomanikule rahaülekande teinud). Kontoomanikule andmete ülekandmise taotluse põhjal pangakonto kohta teabe edastamine kolmandate isikute õigusi ja vabadusi tõenäoliselt ei kahjusta, tingimusel, et isikuandmeid kasutatakse ainult isiklikul eesmärgil (st ainult andmesubjekti kasutatav kontaktaadress või andmesubjekti pangakonto ajalugu).[110] See tekitab

[105] I. Graef, M. Husovec, N. Purtova. Data Portability and Data Control. Lessons for an Emerging Concept in EU Law. - Tilburg Law School Legal Studies Research Paper Series No. 22/2017.
[106] L. Scudiero. Bringing Your Data Everywhere: A Legal Reading of the Right to Portability. – European Data Protection Law Review 2017.
[107] Artikli 29 alusel alustatud Andmekaitse Töörühm. Suunised andmete ülekandmise õiguse kohta, 05.04.2017, lk 11.
[108] L. Urquhart, N. Sailaja, D. McAuley (viide 102).
[109] P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. – Computer Law and Security Review 2017.
[110] Artikli 29 alusel alustatud Andmekaitse Töörühm. Suunised andmete ülekandmise õiguse kohta, 05.04.2017, lk 11.

täiesti uue olukorra, kus ettevõtted peavad üle vaatama oma tehnilise võimekuse.[111] See võib luua koormuse ettevõttele, kel on tehniline võimekus olemas. Samuti on vajalik andmetöötlejatel jälgida, kas andmete ülekandmisel tekib riive kolmandate isikute informatsioonilisele enesemääramisele või mitte.

Seevastu rikutakse kolmandate isikute õigusi ja vabadusi juhul, kui uus vastutav töötleja kasutab nende isikuandmeid muudel eesmärkidel. Näiteks kui vastuvõttev vastutav töötleja kasutab teiste isikute isikuandmeid turustamise eesmärgil, isiku profiili täiendamiseks, sotsiaalse keskkonna ümberkujundamiseks.[112] Näitena võib tuua, et kui andmesubjekti poolt nõutavad andmed puudutavad teavet teiste isikute kohta, võib vastutav töötleja sellisest taotlusest keelduda, sest see võib kahjustada teiste õigusi ja vabadusi. Kui sotsiaalvõrgustikus *Facebook* oleval fotol kuvatakse mitu inimest, siis ei saa seda teisele suhtlusvõrgustiku platvormile üle kanda ühe andmesubjekti nõudmisel, sest see rikuks teiste sellel pildil olevate isikute privaatsust ning andmete ülekandmise õigust.[113] Vastasel korral on selline töötlemine ebaseaduslik, eriti sellisel juhul, kui asjaomaseid kolmandaid isikuid ei teavitata ja nad ei saa andmesubjektidena oma õigusi teostada. Et vältida kahjulikku mõju kolmandatele isikutele, lubatakse uuel vastutaval töötlejal selliseid isikuandmeid töödelda ainult sellises ulatuses, milles taotluse esitanud kasutajal on andmete üle ainukontroll ja neid hallatakse eranditult isiklikel või kodustel eesmärkidel. Lisaks peaksid vastutavad töötlejad kasutama mehhanisme teistelt asjaomastelt andmesubjektidelt nõusoleku saamiseks hõlbustamaks andmete edastamist juhtudel, mil kõnealused isikud soovivad nõusoleku anda. Näiteks kui nad soovivad samuti oma andmeid mõnele teisele vastutavale töötlejale edastada. Selline olukord võib tekkida sotsiaalvõrgustike puhul, kuid vastutavad töötlejad peavad ise otsustama, millist head tava nad järgivad.[114] Siin on jäetud teatud määral tõlgendamisruumi, et otsustada, milliseid viise järgida või kuidas teatud olukordades otsust langetada. Autori hinnangul võib sellistes olukordades tekkida oht kolmanda isiku informatsioonilise enesemääramise osas, eriti juhtudel, kus isikut ei teavitata tema nõusoleku vajalikkusest. Seega võivad tekkida olukorrad, kus andmeid kantakse üle näiteks ühest võrgustikust teise ja kolmandalt isikult ei küsita nõusolekut (näiteks pildid, videod). Kuna see nõuab ettevõtjatepoolset ressurssi, siis võib juhtuda, et nõusolek jäetakse küsimata. Samuti võivad vastutavad töötlejad eeldada, et seaduslik alus on

[111] Andmekaitse Inspektsioon. Mida tähendab andmete ülekandmise õigus? – AKI koduleht, 15.09.2017. Kättesaadav arvutivõrgus: http://www.aki.ee/et/andmekaitse-reform/mida-tahendab-andmete-ulekandmise-oigus
[112] Artikli 29 alusel alustatud Andmekaitse Töörühm. Suunised andmete ülekandmise õiguse kohta, 05.04.2017, lk 12.
[113] A. D. Vanberg, M. B. Ünver. The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? – European Journal of Law and Technology 2017.
[114] Artikli 29 alusel alustatud Andmekaitse Töörühm. Suunised andmete ülekandmise õiguse kohta, 05.04.2017, lk 12.

isikuandmete töötlemiseks olemas, kuigi see nii ei ole. Seetõttu on oluline igas olukorras analüüsida, kas töödeldakse isikuandmeid vastavalt üldmääruses sätestatud nõuetele. Andmete ülekandmise õigus on tekitanud ettevõtetele, kel on olemas vastav tehniline võimekus, suure koormuse ja vastutuse.

Andmete ülekandmise õigust on kritiseeritud, sest see kujutab ohtu pikaajalisele Euroopa Liidu andmekaitse põhiõigusele – isikuandmete turvalisuse õigusele. Individuaalsete taotluste formaat ja ulatus on siiani olnud piiratud, kuid nüüd on seda võimalik teha piiramatus mahus.[115] Andmekaitse Töörühm on selgitanud, et üldmäärusega ei ole ette nähtud mingeid nõudeid andmesubjekti autentimise kohta. Üldmääruses on sätestatud, et vastutav töötleja ei tohiks keelduda meetmete võtmisest andmesubjekti taotlusel tema õiguste kasutamiseks, v.a kui ei ole vaja andmesubjekti tuvastada ja kui saab tõendada, et ei suudeta andmesubjekti tuvastada. Näiteks kasutajakonto puhul piisab autentimiseks kasutajatunnusest ja paroolist.[116] Küsimus on oluline ka nõusoleku puhul: kas taotluse esitanud isik on ikka see sama isik? Autori hinnangul võib olla tuvastamine parooli ja kasutajatunnuse kaudu ebaturvaline. Arvestades häkkerite aina aktiivsemat tegevust ning arenenud oskusi, loob see kindlasti juurde ka rohkem ohtusid. Alles hiljuti oli Eestis juhtum, kus 200 000 eestlase sotsiaalmeedia konto paroolid murti lahti.[117]

Näiteks kui isik häkib andmesubjekti *Hotmail* kontole sisse, siis on tal samuti võimalik näha pilte, videosid, mis on isikul sama süsteemi pilvesüsteemis (*Onedrive*). Kontosid on võimalik turvalisemaks muuta kas nö varu e-maili aadressile meili saatmise teel (kui näiteks isikul on 2 e-maili) või oleks võimalik autentida nö salaküsimuse teel (näiteks kes oli su lapsepõlve parim sõber vms), mida mitmed teenusepakkujad ka kasutavad. Küsimuse vastust ei tohiks olla võimalik häkitud konto alt vaadata ja see võimaldaks paremini isikut tuvastada, kuid see ei ole alati kõige parem lahendus. Autor on seisukohal, et pigem oleks vajalik populariseerida mobiili-ID-d ja teisi mobiilseid autentimisviise, mis tagaksid kõrgema turvalisusetaseme. Seega võib andmete ülekandmise osas tekkida oht, et informatsiooniline enesemääramine ei ole nõusoleku alusel piisaval määral tagatud just isikutuvastamise seisukohalt. Piiramatus mahus andmeid võib minna teisele veebiplatvormile isiku enda teadmata ning seetõttu tekib oht informatsioonilisele enesemääramisõigusele. Samal ajal on keeruline tagada täielikult turvalist

[115] P. Swire, Y. Lagos. Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. – Maryland Law Review 2013.
[116] Artikli 29 alusel alustatud Andmekaitse Töörühm. Suunised andmete ülekandmise õiguse kohta, 05.04.2017, lk 14.
[117] P. Luts. 200 000 eestlase sotsiaalmeedia konto paroolid murti lahti. – ERR. 15.12.2017. Kättesaadav arvutivõrgus: https://www.err.ee/648930/200-000-eestlase-sotsiaalmeedia-konto-paroolid-murti-lahti

isikuandmete töötlemist andmete ülekandmisel. Veebiteenuste kasutamisel jäävad alatiseks alles ohud isikuandmete lekkimisele.

2.2. Nõusoleku andmine teadusuuringute jaoks

2.2.1. Andmesubjekti nõusolek teadusuuringutes

Hetkel kehtiv IKS reguleerib teadustööde jaoks antavat nõusolekut järgnevalt: IKS § 16 lõiked 1-3 selgitavad, et isikuandmeid võib töödelda nõusolekuta teadusuuringu või riikliku statistika vajadusteks üksnes kodeeritud kujul. Tagasikodeerimine on lubatud ainult täiendavate teadusuuringute jaoks ning andmetöötleja peab määrama nimeliselt isiku, kes andmetele juurde pääseb. Andmesubjekti tuvastamist võimaldaval kujul võib nõusolekuta töödelda üksnes juhul, kui pärast tuvastamist võimaldavate andmete eemaldamist ei oleks enam andmetöötluse eesmärgid saavutatavad või oleks nende saavutamine ebamõistlikult raske. Sellisel juhul võib andmeid töödelda, kui on olemas ülekaalukas avalik huvi ning andmesubjekti õigusi ei kahjustata muul viisil. Samuti peavad kasutusele olema võetud organisatsioonilised, füüsilised ja infotehnilised turvameetmed.[118] Seega on siiani olnud vähemalt Eestis võimalik isikuandmeid teadustööde tarbeks töödelda ka ilma andmesubjekti nõusolekuta. Näiteks juhul, kui isikuandmed tagasikodeeritakse täiendavate teadusuuringute jaoks.

Üldmääruse põhjenduspunktis 33 on selgitatud, et teadusuuringute puhul pole isikuandmete kogumise ajaks võimalik määratleda täpselt kõiki teaduslikke eesmärke. Seetõttu peaks andmesubjektidel olema võimalik anda oma nõusolek teatavates uuringuvaldkondades juhul, kui järgitakse selle valdkonna tunnustatud eetikanorme. Isikutel peaks olema võimalik anda oma nõusolek üksnes teatavates teadusuuringu valdkondades või teadusprojektides osades, mis on kavandatud eesmärgiga lubatud ulatuses. Üldmääruse põhjenduspunkt 161 määratleb täpsemini, et kliinilisi uuringuid hõlmavates teadusuuringutes osalemiseks nõusoleku küsimiseks peaks kohaldama Euroopa Parlamendi ja nõukogu määruse nr 536/2014 (15) asjakohaseid sätteid.[119] Isikuandmete kaitse seaduse eelnõu seletuskiri selgitab määrust nr 536/2014 viisil, et tegemist on õigusaktiga, milles käsitletakse inimtervishoius kasutatavate ravimite kliinilisi uuringuid ning statistiline eesmärk tähendab eelkõige kõiki isikuandmete kogumise ja töötlemise toiminguid, mis on vajalikud statistikauuringuteks. Statistiline eesmärk eeldab, et töötlemise tulemuseks on koondandmed, mitte isikuandmed.[120]

[118] Isikuandmete kaitse seadus. – RT I, 06.01.2016, 10.
[119] Euroopa Parlamendi ja Nõukogu määrus 2016/679.
[120] Isikuandmete kaitse seaduse eelnõu seletuskiri. 06.11.2017, lk 18. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_en_9.11.17.pdf.

Isikuandmete kaitse seaduse eelnõu § 6 lõike 1 kohaselt võib andmesubjekti nõusolekuta teadusuuringu või riikliku statistika vajadusteks töödelda andmesubjekti kohta käivaid andmeid eelkõige pseudonüümitud või samaväärset andmekaitse taset võimaldaval kujul.[121] Pseudonüümimise (üldmääruses toodud artiklis 4 punktis 5 mõistena *„pseudonümiseerimine“,* IKS eelnõus toodud mõistena *„pseudonüümimine“*) mõistest arusaamiseks peab lähtuma üldmääruse artikli 4 punktis 5 sätestatut. Eelkõige peab eesmärk põhinema selles, et tagatud on andmesubjektide põhiõigused ja -vabadused.[122] Eesti IKS eelnõus on esile toodud §-s 6 täpsemad nõuded isikuandmete töötlemiseks: välja on toodud kohustus määrata isik, kes saab depseudonüümitud isikuandmetele juurdepääsu; erandid, mil võib isikuandmeid töödeldada viisil, kus isik on tuvastatav jne.[123] Saksamaa föderaalse andmekaitse seaduse §-s 27 on samuti sätestatud erisused ilma nõusolekut küsimata isikuandmete töötlemiseks teadusuuringute, statistika ja ajaloolise uuringu jaoks. Antud paragrahvis pole eraldi välja toodud pseudonümiseerimise mõistet, välja on toodud anonümiseerimise võimalus eriliigiliste isikuandmete töötlemise puhul, kuid on viidatud erinevatele tehnilistele võimalustele, mis peaksid olema kasutusele võetud. Samuti on esile toodud, et vastutav töötleja võib avaldada isikuandmeid juhul, kui andmesubjekt on andnud nõusoleku või kui see on vajalik uurimistulemuste esitamiseks hetkel oluliste sündmuste jaoks.[124]

Andmekaitse Töörühma juhend on samuti kirjeldanud üldmääruse sätteid nõusoleku andmise kohta teadusuuringutes. Töörühma arvates tuleb mõistet *„teadustöö“* tõlgendada eelkõige uurimisprojektina, mis on loodud vastavalt asjakohastele valdkondlikele metoodilistele ja eetilistele standarditele. Täpsemalt pole üldmääruses mõistet defineeritud.[125] Andmepõhise innovatsiooni ja teadustöö edendamine üksikisiku õiguste ja vabaduste austamise tagamiseks on Euroopa digitaalse turu eesmärk. Sarnaselt direktiivile 95/46 tunnistab üldmäärus vajadust teadusuuringute lihtsustamise järele. Teisest küljest rõhutab üldmäärus ka vajadust eetiliste ja vastutustundlike teadusuuringute järele, mis peaks andma andmesubjekti õigustele vajalikud kaitsemeetmed ja austama piiranguid konkreetsetel asjaoludel.[126]

Põhjenduspunkti 33 selgituseks on Töörühm välja toonud, et uurimisprojektid peaksid hõlmama väga täpselt kirjeldatud eesmärki ning kui eesmärgid on ebaselged, siis on programmi

[121] Isikuandmete kaitse seaduse eelnõu. 21.03.2018.
[122] Isikuandmete kaitse seaduse eelnõu seletuskiri. 21.03.2018, lk 15.
[123] Isikuandmete kaitse seaduse eelnõu. 21.03.2018.
[124] The Bundestag. Federal Data Protection Act.
[125] Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 27.
[126] N. Bertels. Scientific research under the GDPR: what will change? - KU Leuven Centre for IT & IP Law 2016. Arvutivõrgus kättesaadav: https://www.law.kuleuven.be/citip/blog/scientific-research-under-gdpr-what-will-change/

täitmine keeruline. Samas lubab põhjenduspunkt 33, et eesmärke võib siiski ka üldisemalt kirjeldada. Juhul, kui töödeldakse eriliigilisi andmeid, siis peab arvestama, et kohaldatakse rangemat tõlgendust ja nõutakse suuremat kontrolli. Lisaks peab vastutav töötleja kohaldama täiendavaid kaitsemeetmeid.[127] Eesti isikuandmete kaitse seaduse eelnõu seletuskiri selgitab, et teatud teadusuuringute puhul on vajalik eelnev Andmekaitse Inspektsiooni või eetikakomitee luba (juhul, kui kasutatakse eriliike või uuring tehakse andmesubjekti tuvastavate andmetega). Loa uuringu teostamiseks annab vastava valdkonna eetikakomitee või AKI, kui eetikakomiteed ei ole loodud. Välja tuleb tuua, et eetikakomitee või Andmekaitse Inspektsiooni luba ei ole vaja, kui viiakse andmed mittetuvastavale kujule. Luba on vaja siis, kui kogu analüüs põhineb jooksvalt andmesubjekti tuvastada lubavatel isikuandmete eriliikidel.[128] Kui eesmärgid jäävad teadustöö raames ebatäpseks, siis ei pruugi andmesubjekti poolt antud nõusolek tagada tema informatsioonilist enesemääramisõigust. Eesmärkide ebaselgus loob olukorra, kus isik ei ole nõusoleku andmise hetkel teadlik, millistel eesmärkidel tema isikuandmeid töödeldakse ning kuhu need andmed sattuda võivad. Sellisel juhul võib andmesubjektil kaduda kontroll oma isikuandmete üle ning nõusolek ei ole kehtiv. Seetõttu on oht, et teatud juhtudel ei ole täielikult tagatud andmesubjekti informatsiooniline enesemääramisõigus, sest andmed võivad sattuda kohtadesse, millele andmesubjekt ei ole oma nõusolekut andnud. Teadustöö eesmärk ja olemus on väga olulised, kuid siin peab arvestama ka andmesubjektide isikuandmete kaitsega.

Nõusoleku andmise osas teadusuuringute jaoks on erinevaid arvamusi. Leitakse, et uus üldmäärus tugevdab koostööd ja läbipaistvust andmetöötlejate ja järelevalveasutuste vahel, mis peaks looma integreerituma Euroopa Liidu andmekaitse süsteemi. Samal ajal võib see luua olukordi, kus nõusolek ei ole kehtiv. Lisaks viitab üldmäärus esimest korda eetiliste standardite järgimisele, kuna see on oluline osa uurimismenetluse seaduslikkusest. Üldmäärusega kaasnevad muudatused peaksid optimistlikult struktureerima Euroopa teadusruumi.[129]

Digitaalse ühtse turu eesmärk on parandada andmete jagamist kogu Euroopa Liidus, mis lihtsustab piiriüleste tervishoiuteenuste ja teadusuuringute läbiviimist. Üldmäärus hõlbustab meditsiinilist uuringut, välja arvatud juhul, kui teadusuuringuid ei tehta avalikes huvides. Sellisel juhul toovad anonüümsuse nõuded kaasa tõsisema anonüümistumise või nõusoleku küsimise. Tõenäoliselt hakkab olema rohkem projekte, mis nõuavad nõusoleku küsimist.[130] Üldmäärus läheb kaugemale praegusest seadusandlusest ning nõuab organisatsioonidele

[127] Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 27, 28.
[128] Isikuandmete kaitse seaduse eelnõu seletuskiri. 21.03.2018, lk 15.
[129] G. Chassang. The impact of the EU general data protection regulation on scientific research. – Ecancermedicalscience 2017.
[130] J. M. M. Rumbold. B. Pierscionek. The Effect of the General Data Protection Regulation on Medical Research. – Journal of Medical Internet Research 2017.

kõrgemaid standardeid andmete töötlemisel, aga need kõrgemad standardid peavad olema kooskõlas parimate tavade ja eetikanormidega. Organisatsioonilised meetmed peaksid olema tõhusad ja kogu organisatsiooni sisseehitatud, kuid üldmäärus põhineb suuresti läbipaistvusel ja usaldusel suhtes riiklike ja rahvusvaheliste õigusaktidega.[131] Teadusuuringute puhul ei pea olema isikuandmete töötlemiseks õiguspäraseks aluseks nõusolek. Üldmäärus võimaldab teadlastel töödelda tundlikke andmeid ja piiratud tingimustel edastada isikuandmeid kolmandatele riikidele, kus ei pakuta piisavat kaitset. Nende erandite kasutamiseks peavad teadlased rakendama asjakohaseid kaitsemeetmeid kooskõlas tunnustatud eetiliste standarditega.[132] Kindlasti loob see ühtsemat digitaalset andmevahetuse turgu kogu Euroopas, kuid samal ajal tekitab see erinevaid ohtusid isikuandmetele ning ka informatsioonilisele enesemääramisõigusele, kui isikuandmeid edastatakse näiteks kolmandatesse riikidesse ning teada pole info kolmandate riikide asutuste turvameetmete kohta. Sellisel juhul ei saa garanteerida andmesubjektidele piisavalt kõrget isikuandmete kaitsetaset.

Teadusuuringute erandid andmekaitsealastes õigusaktides peaksid võimaldama luua kontekstipõhist normatiivset raamistikku, milles saab arvesse võtta eriliigiliste isikuandmete kasutamise eripärasid meditsiinilises uuringus. Siiski on vaja täiendavaid interdistsiplinaarseid teadusuuringuid, et teha kindlaks, millal eemaldumine nõusolekust kui õiguslikust alusest on vajalik ja proportsionaalne andmete meditsiinilise uurimistöö kontekstis ning milliseid tehnoloogilisi meetmeid tuleks kehtestada.[133] Samuti peaks andmesubjektidel olema võimalik saada põhjalik uurimisplaan, et neil oleks võimalik teadvustada uuringu põhimõtteid enne, kui nad nõustuvad isikuandmete töötlemisega. Seda tuleb teha sellisel juhul, kui eesmärgid ei ole piisavalt täpselt välja toodud. Selles uurimisplaanis tuleks selgelt välja tuua uuritavad küsimused ja töömeetodid. Uurimisplaan võiks aidata kaasa ka artikli 7 lõike 1 järgimisele, kuna vastutavad töötlejad peavad näitama, milline teave oli andmesubjektidele nõusoleku andmise ajal kättesaadav ning seeläbi on võimalik tõendada nõusoleku kehtivust.[134]

Oluline on meeles pidada, et kui andmetöötluse seadusliku baasina kasutatakse nõusolekut, peab andmesubjektil olema võimalus see nõusolek tagasi võtta. Andmekaitse Töörühm märgib, et nõusoleku tagasivõtmine võib kahjustada teaduslikke uuringuid, mis nõuavad üksikisikutega seostatavaid andmeid. Samas on üldmääruse üks olulisemaid printsiipe, et nõusolekut võib

[131] M. Goddard. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. - International Journal of Market Research 2017.
[132] G. Maldoff. How GDPR changes the rules for research. – The International Association of Privacy Professionals 2016. Arvutivõrgus kättesaadav: https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/
[133] M. Mostert, A. L. Bredenoord, M. Biesaart and J. van Delden. Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. – European Journal of Human Genetics 2016.
[134] Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 28, 29.

tagasi võtta ja vastutavad töötlejad peavad seda sellega leppima - teadusuuringutele ei tehta antud juhul erandit. Kui vastutav töötleja saab nõusoleku tagasivõtmise taotluse, peaks ta isikuandmed kohe kustutama või anonüümseks tegema, kui ta soovib andmete kasutamist uuringu eesmärgil jätkata.[135] Õiguslikult keeruline olukord võib ka tekkida siis, kui täiskasvanud või 16-18-aastased keelduvad isikuandmete töötlemisest. Kui vastutavad töötlejad ei ole varem saanud lapselt nõusolekut, saavad nad tööd jätkata lapse 18. aastaseks saamisel ainult juhul, kui alternatiivne õiguslik alus on neile kättesaadav. Siin peab töötlemine olema õiglane. Hinnates, kas jätkuv töötlemine on õiglane, tuleks täiendavalt arvestada: kas selle alternatiivse õigusliku aluse kasutamine töötlemise aluseks on avalikult ja läbipaistvalt edastatud nii seaduslikule esindajale ja andmesubjektile. Vältimaks võimalust, et andmekaitseinspektorid leiavad ilma õigusliku aluseta isikuandmete töötlemise pärast 18. eluaastat (või varem), oleks soovitatav võtta kasutusele tõhusa kommunikatsiooni meetodid.[136]

Nõusoleku tagasivõtmine teadustööde raames loob suurel määral ebakindlust isikuandmete töötlejatele. See võib rikkuda teadustöö tulemusi või muuta teadustöö väärtusetuks ka eelmainitud olukorras, kus andmesubjekt saab 18 ning pole enam nõus isikuandmete töötlemisega. Samuti peab rõhutama, et kui andmesubjektil on õigus nõusolek tagasi võtta, siis kannatab seetõttu teadustöö valim.

Väikeriigi jaoks on väga oluline heal tasemel teadlaskond ning teadust ja ülikoole peetakse ühiskondliku progressi peamiseks edasiviivaks jõuks.[137] Võttes arvesse seda, kui olulisel kohal on teadusuuringud (Eesti ühiskonna arengu kontekstis) ja mil määral võib mõjutada isikuandmete tagasivõtmise võimalus teadusuuringute edukust, siis tuleks analüüsida, kas riive on proportsionaalne või mitte. Autori hinnangul tuleks iga juhtumi puhul kaaluda riivet teadusuuringu teostajale ning andmesubjekti informatsioonilise enesemääramise suhtes. Riive võib teatud kontekstis olla ebaproportsionaalne teadusuuringutele, sest kogu valim ja tulemused võivad ohtu sattuda, kui andmesubjekt otsustab nõusoleku tagasi võtta. Seega võib kogu teadustöö kaotada oma tähenduse ning väärtuse, kuid see oleneb kindlasti konkreetsest olukorrast. Samas võib nõusoleku tagasivõtmise võimaluse olemasolu omakorda pärssida teadusuuringute teostamist ning üldisemalt ühiskonna arengut.

Kui analüüsida laiemalt nõusoleku tähtsust terviseandmete töötlemisel Eesti näitel, siis on ilmselt oluliseks kohaks Digilugu.ee ehk e-tervise keskkond. E-tervises on võimalik

[135] Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 29.
[136] M. J. Taylor, E. S. Dove, G. Laurie, D. Townend. When can the Child Speak for Herself? The Limits of Parental Consent in Data Protection Law for Health Research. – Medical Law Review Vol. 0, 2017.
[137] M. Maidla. Milline on teaduse tähtsus ja sotsiaal-majanduslik mõju? – Sirp 2017.

keelata/sulgeda juurdepääs teatud terviseandmetele.[138] E-tervise üks eesmärkidest on luua võimalus andmete kasutamiseks teadusuuringute jaoks.[139] Näiteks, kui tegemist on psühhiaatrilist abi vajava isikuga, kas sellisel juhul ei võiks olla arsti diskretsiooniotsus isikuandmetele ligi pääseda või mitte. Kui isik on ebastabiilne, siis ei pruugi ta teha kõige ratsionaalsemaid ja tema heaolule vastavaid otsuseid. Samuti peaks hindama, kas isik on oma tervisliku seisundi tõttu piisavalt pädev nõusolekut andma ehk jagama terviseandmeid meditsiinitöötajaga. Selliseid olukordi võib olla keeruline määratleda, millal peaks eelkõige diskretsiooniõigus olema patsiendil ja millal raviarstil, kuid see on kindlasti teema, mida peaks antud kontekstis rohkem analüüsima. Samal ajal võib esile tuua, et hetkel on e-tervise keskkonnas kõik tervise kohta olemasolevad isikuandmed kättesaadavad ehk märksõnaga „arstile avatud" (kui just eriarst ei ole ise piiranud nende kättesaadavust). Sellisel juhul ei ole isik oma nõusolekut just nende isikuandmete jaoks andnud. Tegemist peaks olema aktiivse tegevusega antud nõusolekuga. Seega peaksid algselt kõik tervise kohta käivad andmed olema suletud arstidele ning alles siis peaks isikul olema võimalus need nähtavaks teha. Siin tuleb jällegi esile, et isikul pole võimalik end informatsiooniliselt määrata, sest osad otsused on tehtud tema enda eest. Samal ajal võib sellisel viisil isikuandmete töötlemiseks olla seaduslikuks aluseks isikuandmete töötlemine andmesubjekti elu ja tervise huvides.

2.2.2. Pseudonümiseerimise tähendus

Pseudonümiseerimise mõistest arusaamiseks peab lähtuma üldmääruse artikli 4 punktis 5 sätestatust *(„pseudonümiseerimine" – isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga, tingimusel et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava füüsilise isikuga seostamise vältimise tagamiseks võetakse tehnilisi ja korralduslikke meetmeid[140]*). Eelkõige peab eesmärk seisnema selles, et tagatud on andmesubjektide põhiõigused ja -vabadused.[141] Uue isikuandmete kaitse seaduse eelnõu §-i 6 lõikes 1 on samuti välja toodud, et *„andmesubjekti nõusolekuta võib teadus-, ajaloouuringu või riikliku statistika vajadusteks isikuandmeid töödelda eelkõige pseudonüümitud või samaväärset andmekaitse taset võimaldaval kujul. Enne isikuandmete üleandmist teadus- või ajaloouuringu või riikliku statistika vajadustel töötlemiseks asendatakse isikuandmed pseudonüümitud või samaväärset andmekaitse taset võimaldaval kujul andmetega"*. Samas on lõike 2 alusel võimalik andmeid

[138] Patsiendi õigused. Patsiendiportaal. Kättesaadav arvutivõrgus: http://www.e-tervis.ee/index.php/et/2012-07-22-09-19-35/patsiendiportaali-voimalused/patsiendi-oigused
[139] Riigikontrolli aruanne Riigikogule. Riigi tegevus e-tervise rakendamisel, 17.01.2014.
[140] Euroopa Parlamendi ja Nõukogu määrus 2016/679.
[141] Isikuandmete kaitse seaduse eelnõu seletuskiri. 21.03.2018, lk 15.

depseudonüümida, kui on vajalik teha täiendavaid teadus- või ajaloouuringuid või teostada riiklikku statistikat. Lõikes 3 on selgitatud, et tuvastavaid andmeid võib ilma nõusolekuta töödelda, kui peale andmete eemaldamist pole eesmärkide saavutamine võimalik või ülekaaluka avaliku huvi korral või ei muudeta andmesubjekti kohustuste mahtu ega kahjustata muul viisil ülemäära andmesubjekti õigusi.[142] AKI on kommenteerinud, et teatud paindlikkus isikuandmete kasutamisel teadusuuringuteks on vajalik.[143] Võimalikud on olukorrad, kus andmesubjektil pole sel eesmärgil kontrolli oma isikuandmete üle ning võib tekkida riive isiku õigusele end informatsiooniliselt määrata. See võib juhtuda sellises olukorras, kus depseudonümiseeritakse andmeid, et teostada täiendavaid teadusuuringuid.

AKI on välja toonud, et Eestis puudub hetkel konkreetne õiguslik alus pseudonümiseerimise jaoks, sest selle raames toimub samuti isikuandmete töötlemine, kuna isikuandmed viiakse sellele kujule nende algkujust.[144] Samas on pseudonümiseerimise puhul ikkagi oht, et andmeid võidakse depseudonümiseerida. Seeläbi on võimalik tuvastada isik, kes on nende andmetega seotud, mistõttu võivad tekkida olukorrad, kus teatud isikuandmetega on võimalik seostada konkreetset andmesubjekti. Seletuskirjas[145] on märgitud, et isikustamata kujul olevatele andmetele ei kohaldata isikuandmete kaitse üldmäärust. Samuti on lisatud, et anonüümse andmeanalüüsi korral ei tule järgida isikuandmete kaitse õiguse reegleid, kuid pseudonümiseeritud või mõnel muul viisil andmesubjekti mittetuvastataval kujul tuleb järgida isikuandmete kaitse üldmääruse norme.

Oluline on mõista, et antud valdkonnas ei ole nullriski olemas ja hetkel on võetud suund riskipõhisele lähenemisele andmete töötlemise osas. Selles valdkonnas on vaja teostada rohkem uurimusi, et täielikult mõista erinevate töötlemiskategooriate ja erinevate keskkonnakomponentide koosmõju: andmeid ja infrastruktuuri. Üldmääruses leiduv pseudonüümiseerimise määratlus on eksitav, sest see ei viita riskidele, mis on seotud isikuandmete salvestuste sidumisega ühes või enamas andmekogumis.[146] Pseudonümiseerimine loob teatud ohtusid andmesubjektide eriliigiliste isikuandmete osas, kuna täiendava teabe olemasolul on võimalik isikuandmeid konkreetse füüsilise isikuga seostada. Seeläbi on võimalik tuvastada isik, kes on nende andmetega seotud. Pseudonümiseerimise puhul on autori hinnangul oluline andmesubjektide teavitamiskohustus,

[142] Isikuandmete kaitse seaduse eelnõu. 21.03.2018.
[143] Andmekaitse Inspektsioon. Andmekaitse Inspektsiooni täiendavad seisukohad uue andmekaitseõiguse kontseptsiooni asjus 22.06.2017.
[144] Andmekaitse Inspektsioon. IKS eelnõule arvamuse avaldamine 21.12.2017.
[145] Isikuandmete kaitse seaduse eelnõu seletuskiri. 21.03.2018, lk 15.
[146] S. Stalla-Bourdillon, A. Knight. Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. – Wisconsin International Law Journal 2016.

mis annaks andmesubjektile arusaama, et teatud juhtudel on võimalik, et isikuandmeid töödeldakse ka isikustatud kujul.

On oluline mõista, et antud valdkonnas ei ole nullriski olemas ja hetkel on võetud andmete töötlemise osas riskipõhisele lähenemisele. Selles valdkonnas on vaja teostada rohkem uurimusi, et täielikult mõista erinevate töötlemiskategooriate ja keskkonnakomponentide koosmõju: andmeid, infrastruktuuri ja inimesi. Vajalik on pseudonümiseeritud andmete kontuurid selgelt piiritleda, kuna üldmääruses leiduv pseudonüümiseerimise määratlus on eksitav, sest see ei viita riskidele, mis on seotud isikuandmete salvestuste sidumisega ühes või enamas andmekogumis.[147] Samuti on kaitsemeetmete kirjeldus jäänud ebatäpseks ning selle mõiste sisustamine delegeeritakse tagasi liikmesriikidele. Harmoniseerimist Euroopa Liidu liikmesriikide vahel võib takistada see, et Euroopa Liidus võivad liikmesriigiti tulla erinevused. See võimaldab mõnedel riikidel olla suurandmete puhul lubavam, teistel piiravam. See muudab tegutsemise keerulisemaks ettevõtete ja organisatsioonide jaoks, kes tegutsevad mitte ainult ühes, vaid mitmes Euroopa Liidu liikmesriigis. See kehtib eriti veebipõhiste teenusepakkujate kohta, kes soovivad pakkuda oma teenuseid kogu Euroopa Liidus. Euroopa Liidu poliitikakujundajad pidasid ilmselt innovaatiliste e-kaubanduse ja suurandmete ettevõtete uuenduslikke panuseid vähem tähtsaks võrreldes vajadusega parandada EL-i kodanike privaatsuse kaitset.[148] Autor nõustub eelnevate väidetega, et tehniliste nõuete rakendamises võib tekkida mitmeid erinevaid praktikaid, mis tõesti võivad luua erinevaid kaitsetasemeid liikmesriikides ning põhjustada raskusi ettevõtetele.

2.3. Lapse nõusolekule kohaldatavad nõuded

2.3.1. Lapse isikuandmete kaitse tagamine üldmääruse alusel

Alates 1995. aastast on alaealistele kohaldatavad direktiivis 95/46/EÜ sätestatud vanusepõhised andmekaitsenõuded, kuid laste isikuandmetele ei ole direktiivis erilist tähelepanu pööratud.[149] Andmekaitsedirektiiv ei maini eraldi laste õigusi, vaid esitab pigem üldise deklaratsiooni, et isikuandmeid peab töötlema õiglaselt. Sellises kontekstis võib tõlgendada, et olulisel kohal on ka andmesubjekti vanus ja arusaamise tase, kuid praktikas pole piisavalt kohtulahendeid, mis aitaksid seda tõlgendada.[150] EL-i üldmäärus on praegust olukorda oluliselt muutnud ja laste[151]

[147] *Ibid.*
[148] V. Mayer-Schonberger, Y. Padova. Regime change? Enabling big data through Europe's new data protection regulation. – The Columbia Science and Technology Law Review 2016.
[149] M. Macenaite, E. Kosta. Consent for processing children's personal data in the EU: following in US footsteps? – Information and Communication Technology Law 2017.
[150] J. Carr. The position of children and their rights under the GDPR. – The London School of Economics and Political Science. Media Policy Project 2017.
[151] Laps üldmääruse tähenduses on isik, kes on alla 16. aastane või alla vanuse, mis on siseriiklikult sätestatud.

isikuandmete kaitset efektiivsemaks reforminud. Üldmäärus tunnistab selgesõnaliselt, et lapsed vajavad rohkem kaitset kui täiskasvanud. Nagu üldmääruse põhjenduspunktis 38 on selgitatud, siis väärivad lapsed erilist kaitset, sest nad võivad olla vähem teadlikud riskidest, tagajärgedest, kaitsemeetmetest ja nende õigustest seoses isikuandmete töötlemisega (eriti veebis).[152] Andmekaitse Töörühma arvates on olulisel kohal laste nõusoleku temaatika, kuna lapse ja andmetöötleja vahel valitseb suur ebavõrdsus. Lapsed ei pruugi olla piisavalt võimekad, et oma andmete töötlemisele teadlikult ja põhjalikult vastu vaielda. See puudutab ka erilist kaitset vajavaid elanikkonnarühmi, näiteks vaimuhaigeid, varjupaigataotlejaid või eakaid patsiente.[153]

Üldmääruse järgi muutub lapse isikuandmete töötlemine keerulisemaks ning peaks suuremal määral tagama lapse isikuandmete kaitset. Üldmääruse artikkel 8 sätestab, et infoühiskonna teenuste pakkumine otse lapsele ja seoses sellega isikuandmete töötlemine on seaduslik ainult juhul, kui laps on vähemalt 16-aastane. Kui laps on noorem kui 16, siis on vajalik saada nõusolek isikult, kes on lapse suhtes vanemlikult vastutav. Liikmesriikideil on võimalik sätestada madalam vanus, kuid see ei tohi olla vähem kui 13 aastat. Samuti peab vastutav töötleja tegema mõistlikke jõupingutusi selleks, et kontrollida, kas loa andnud isikul on selleks õigus.[154] Tänapäeval on aina rohkem lapsi erinevates veebikeskkondades. Uuringute järgi on maailmas üks kolmest internetikasutajast alaealine.[155]

Suhtlusportaalides võib kohata piinlikkust tekitavaid pilte varateismelistest, kes üksteist hindavad, kiidavad, laidavad ning need noored ei mõtle sellele, kes nende isikuandmeid lisaks sõpradele töödelda võib. Samuti ei mõelda sellele, kas ka 10 aasta pärast on selliste andmete kättesaadavus jätkuvalt nende huvidega kooskõlas.[156] Andmekaitse Inspektsioon on selgitanud, et erilist tähelepanu vajab internetis toimuv, kuna sisuliselt ei vastuta keegi seal andmete avaldamise õiguspärasuse eest. Sellest tulenevalt peab rohkem tõstma nii laste kui ka nende vanemate/seadluslike esindajate teadlikkust. Põlvkondadevahelised erinevused meedia kasutamisel ning mõtestamisel on suured ning sageli puudub seaduslikul esindajal ülevaade lapse meediatarbimisest (seda eriti interneti puhul). Samuti pole täiskasvanud alati pädevad kasutama või selgitama meedianähtusi.[157] Täiskasvanud toetavad laste isikuandmete kaitsmist.

[152] M. Macenaite, E. Kosta (viide 149).
[153] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 04.04.2017, page 9.
[154] Euroopa Parlamendi ja Nõukogu määrus 2016/679.
[155] S. Livingstone, J. Carr, J. Byrne. "One in Three: Internet Governance and Children's Rights." - Global Commission on Internet Governance Paper Series 2015.
[156] M. Männiko, lk 186.
[157] Andmekaitse Inspektsioon. Laste õigused ja isikuandmete töötlemine 2013.

Seda näitab ka Eurobaromeetri uuring, mille kohaselt uskus 95% eurooplastest, et *„alaealisi isikuid tuleks isikuandmete kogumisest ja avalikustamisest eriliselt kaitsta“* ja 96% arvasid, et *„alaealisi tuleks hoiatada isikuandmete kogumise ja avalikustamise tagajärgede eest“*.[158]

Andmekaitse Töörühm on samuti selgitanud nõusolekualases juhendis mitmeid olulisi artikleid. Seoses vanemliku vastutuse nõusoleku temaatikaga ei määratle üldmäärus praktilisi viise vanema nõusoleku saamiseks ega selle kindlakstegemiseks. Seepärast soovitab Töörühm proportsionaalset lähenemisviisi, mis on kooskõlas üldmääruse andmete minimaliseerimise põhimõttega. Proportsionaalne lähenemine võib olla piiratud hulga teabe saamine, näiteks vanema või seadusliku esindaja kontaktandmed. Mõistlikud viisid kontrollimaks kasutaja vanust kui ka lapse nimel nõusolekut omava vanemliku vastutusega seotud isiku nõusolekut võivad sõltuda andmete töötlemisest ja olemasolevast tehnoloogiast. Madala riskiga juhtudel võib vanemliku vastutuse kontrollimine ka e-posti teel olla piisav. Kõrge riskiga juhtumitel võib olla asjakohane küsida täiendavaid tõendeid, nii et vastutav töötleja suudab teavet kontrollida ja seda säilitada.[159] Segadust tekitab see, mille järgi peaks täpsemalt andmetöötleja hindama, millal on tegemist madala riski juhtumitega ja millal kõrge riskiga. Üldmääruse artikkel 35 lõige 3 loetleb juhtumid, millal on tegemist kõrge riskiga: kui töödeldakse eriliigilisi isikuandmeid, kui tehakse süstemaatilisi, ulatuslikke hindamisi ning ulatuslikku süstemaatilist jälgimist. AKI on lisanud, et see nimekiri pole ammendav ning igal eri juhtumil peaks vastutav töötleja hindama, kas tegemist võib olla kõrge riski juhtumiga.[160] Seega tuleks analüüsida erinevaid olukordi juhtumipõhiselt ning langetada otsus vastavalt olemasolevatele juhistele.

Isikuandmete kaitse seaduse eelnõusse on lisatud eraldi säte (IKS eelnõu § 8) lapse isikuandmete töötlemise kohta, mis kannab edasi üldmääruses sätestatud mõtet. Eesti puhul on vanuse alampiiriks hetkel pandud 13 aastat. Antud §-i lõikes 2 on veel välja toodud, et kui laps on noorem kui 13-aastane, on isikuandmete töötlemine lubatud üksnes sellisel juhul ja sellises ulatuses, milleks on nõusoleku andnud lapse seaduslik esindaja.[161] Isikuandmete kaitse seaduse eelnõu seletuskiri selgitab, et lastele peab rakenduma eriline kaitse, eriti isikuandmete kasutamisel turustuse eesmärgil, isiku või kasutajaprofiili loomiseks ning otse lastele pakutavate teenuste kasutamise puhul. Vanemliku vastutuse kandja nõusolekut ei ole vaja

[158] European Commission. Attitudes on Data Protection and Electronic Identity in the European Union. – Special Eurobarometer 359 2011.
[159] Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 26.
[160] Andmekaitse Inspektsioon. Mis on andmekaitsealane mõjuhinnang? – AKI koduleht, 09.10.2017. Kättesaadav arvutivõrgus: http://www.aki.ee/et/andmekaitse-reform/mis-andmekaitsealane-mojuhinnang.
[161] Isikuandmete kaitse seaduse eelnõu. 21.03.2018.

seoses lastele otse pakutavate nõustamisteenustega.[162] Seletuskiri rõhutab, et edaspidi suureneb lastevanemate vastutus lapse isikuandmete töötlemisel internetikeskkonnas (võib hõlmata kasutajaprofiili loomist, isikuandmete kogumist, otseturustust) ning positiivne mõju peaks ilmnema ka isikuandmete kuritarvitamise võimaluste vähenemises internetikeskkonnas, mis lisaks kuritegelikule tegevusele hõlmab ka sotsiaalseid probleeme (nt libakontod, veebikiusamine). Samas ei saa õiguslik regulatsioon välistada olukordi, kus laps valetab oma vanuse kohta. Statistikaameti andmetel elas Eestis 1. jaanuari 2017 seisuga 188 677 alla 13-aastast last.[163]

2.3.2. Lapse vanuse kontrollimine

Eesti puhul on kindlasti oluline märkida, et alaealiste vanuse määramise osas on olnud erimeelsusi (milline on õige eluiga, et hinnata isiku suutlikkust anda ise oma nõusolek infoühiskonna teenuse pakkujatele). Algses isikuandmete kaitse seaduse eelnõus oli märgitud eluaasta piiriks 14.[164] Andmekaitse Inspektsioon kirjutas eelnõule arvamuse avaldamises, et soovitab jätkuvalt jääda 13 eluaasta piiri juurde, sest karistusõigusega puudub seos (sealt on tuletatud 14 eluaasta piir) ning tõi näitena, et Ameerika Ühendriikide õigusest tulenevalt kasutavad kõik suuremad rahvusvahelised teenusepakkujad 13 eluaasta piiri.[165] Viimases isikuandmete kaitse seaduse eelnõus on jäädud 13. eluaasta piirile.[166] Näiteks on Saksamaa ning Holland hetkel kehtestanud vanuse alampiiriks 16 aastat, kuid Rootsi, Hispaania, Poola, Iirimaa on seadnud vanusepiiriks 13 aastat.[167]

Liikmesriikides saavad vanusepiirid olema väga erinevad. Esile on toodud, et kui lubada liikmesriikidel sätestada vanusepiir 13-16 eluaastat, on see kontseptuaalselt ebaühtlane. Üldmäärus peaks juhinduma ekspertide nõuannetest laste võimekuse kohta, mitte lähtuma sellest, et vanusepiirangud peaks kehtestama liikmesriigid vastavalt enda eelistustele. Euroopa Komisjon või liikmesriikide järelevalveasutused peaksid sponsoreerima teadusuuringuid laste osas, eelkõige eraelu puutumatust käsitlevate teadete osas ning nende suutlikkusega mõista eraelu puutumatuse teateid. Ühtse nõusoleku künnise kehtestamine kõikides liikmesriikides

[162] Isikuandmete kaitse seaduse eelnõu seletuskiri. 21.03.2018, lk 17.
[163] Isikuandmete kaitse seaduse eelnõu seletuskiri. 21.03.2018, lk 54-55.
[164] Isikuandmete kaitse seaduse eelnõu. 06.11.2017.
[165] Andmekaitse Inspektsioon. IKS eelnõule arvamuse avaldamine 21.12.2017.
[166] Isikuandmete kaitse seaduse eelnõu. 21.03.2018.
[167] E. Lievens, I. Milkaité. Age of consent in the GDPR: updated mapping of recent national guidance and proposals. – Better Internet for Kids 16.08.2017. Arvutivõrgus kättesaadav: https://biblio.ugent.be/publication/8528973/file/8528974.pdf

tooks kaasa lisaväärtuse riikidevahelistele teenustele.[168] Autori hinnangul oleks samuti mõistlik läbi viia uuringuid Eesti noorte seas, testida nende teadmisi ja arusaamisi andmekaitsest just erinevates vanusegruppides. See annaks võimalikult objektiivse lähtealuse hindamaks, milline vanus oleks kõige mõistlikum.

Kritiseeritud on vanuse kriteeriumi ebasobilikkust tänapäeva ühiskonnas. Inimesed arenevad erinevalt ja paljud inimesed küpsevad varasemas vanuses kui minevikus. Üldise vanusemäära paikapanek oli ilmselt keeruline ning seetõttu otsustati, et lapse eluiga on jäetud iga liikmesriigi enda otsustada.[169] Vanusepiirangu kehtestamine rikub laste õiguste konventsiooni põhimõtteid. Nooremad lapsed ei pruugi tõesti aru saada nende veebipõhiste tegevuste tagajärgedest ja andmekaitse riskidest, siis võivad teismelised olla neist rohkem teadlikud (isegi rohkem kui nende vanemad) või isegi kasutada sotsiaalvõrgustikke olukordades, kus neil tekivad probleemid ja neile otsitakse lahendust. Teismeliste jaoks on internet väärtuslik uudiste allikas ning tõhus vahend kodanikuühiskonna ja keskkonnaküsimustes osalemiseks. Üldmäärus kehtestab nõude, et igasugune teave ja suhtlemine, kui see on adresseeritud lapsele, tuleks täpsustada selges ja lihtsas keeles, mida laps suudab mõista.[170]

Esitatud on ettepanek, et vajalik oleks kehtestada erinevad vanusepiirangud andmekogumise valdkondade suhtes. Võiks luua standardid, mis võtavad arvesse laste haavatavust konkreetses tegevuses või sektoris. Kui liikmesriigid otsustavad vanusepiiri 13 eluaasta juurde alandada, võiksid erinevate valdkondade tegevusjuhendid seda vanusepiiri ületada ja pakkuda rangemat kaitset konkreetsete juhtumite puhul. Igal juhul peaks kõige sobivama vanusepiiri valimine teatud sektorite puhul põhinema ulatuslikel empiirilistel tõenditel ja lastega konsulteerimisel.[171] Autori hinnangul väärib kaalumist mõte, et kehtestada eri valdkondade pinnalt erisused (nt lastele suunatud suhtlusplatvormid, mänguplatvormid jne). Samas on jällegi raske määratleda, milline oleks õige vanus erinevate valdkondade puhul ning milliste kriteeriumite alusel seda hinnata. Autori arvates oleks üheks lahenduseks olukord, kus lapsevanem annab ühe nõusoleku, mis on universaalne kõikide infoteenuste pakkujate osas ning lubab alaealisel edasiselt ise otsustada, kuhu ta oma andmeid annab. See tagaks olukorra, kus ei oleks vajalik pidev nõusoleku küsimine ning lapsel oleks võimalik teenusepakkujale esitada näiteks digitaalselt allkirjastatud nõusolekuankeet. Jällegi võib tekkida oht, et lapsevanem pole teadlik, mis

[168] T. Bräutigam, S. Miettinen. Data Protection, Privacy and European Regulation in the Digital Age. – Unigrafia OY, Helsinki 2016.
[169] P. Blume (viide 46).
[170] D. Krivokapic, J. Adamovic. Impact of General Data Protection Regulation on Children's Rights in Digital Environment. – Belgrade Law Review No.3 2016.
[171] M. Macenaite, E. Kosta (viide 149).

saitidele alaealine kontod on teinud ja milliseid isikuandmeid edastanud. Sellise lahenduse puhul on olulisel kohal lapsevanema ja tema lapse omavaheline usaldussuhe. Võib juhtuda, et üldmääruse mõte selles osas, et lapsevanem oleks kaasatud lapse isikuandmete jagamisse, läheb sellises lahenduses kaduma, kuid see tagaks nõusoleku andmise lihtsustamise ja annaks lapsele rohkem võimalusi end informatsiooniliselt määrata.

Üldmääruse artikli 8 rakendamine annab EL-ile võimaluse lahendada erinevaid väljakutseid seoses vanuse kontrolli meetoditega. EL peaks uurima innovaatilisi ja tõhusaid vanuse kontrollimise mehhanisme tagamaks üldmääruse selgemat rakendamist. Lapsevanema nõusoleku kontrollimeetodite kindlaksmääramisel võib EL järgida Ameerika Ühendriikide eeskuju selles osas, et julgustada erinevaid tööstussektoreid pakkuma tõhusaid, vastuvõetavaid ja sektori jaoks kohandatud lahendusi.[172]

Suurim praktiline väljakutse on tagada, et lapse vanust ja seaduslike esindajate nõusolekut oleks võimalik veebisaidil kontrollida. Siiani ei ole olnud kindlaid ja sobivaid mehhanisme lapse vanuse kontrollimiseks veebis. Lapsed on võimelised kõrvale hoidma vanuse kontrollimise mehhanismidest. Näiteks sellisel juhul, kui nad annavad valeinfot oma vanuse kohta. Seetõttu peaksid nõusoleku kontrollimise mehhanismid olema nii tõhusad kui ka hõlpsasti kasutatavad ning kinni peaks pidama põhilistest andmekaitse põhimõtetest (andmete minimaalsus, eesmärkide piiramine, andmete piisavus ja asjakohasus).[173] Vanuse kontrollimine tekitab palju tundlikke küsimusi, mis on seotud laste sõnavabadusega. Täiuslik vanuse kontroll on teostumatu eesmärk, kuid on oluline, et ei hakataks kasutama lahendusi, mis annaksid vale turvatunde kas vanematele või noortele, kes kasutavad suhtlusvõrgustikke. Sotsiaalvõrgustike vanuse kontrollimise viiside kehtestamise ettepanekud tõstatavad palju tundlikke küsimusi, millel võib olla suur mõju üksikisikute privaatsusele.[174]

Samuti on rõhutatud, et ettevõtetele kehtestatud kontrollinõude rakendamine võib rikkuda andmete minimaliseerimise põhimõtet. Ettevõtted peaksid nõudma ainult teavet, mida nad tõesti vajavad kontrolli ja teenuse osutamiseks. Seoses sellega võib isikut tõendava dokumendi nõudmisega tekkida liialt suur riive privaatsusele, seega peaks lapsel olema võimalik oma vanust teiste vahenditega tõestada.[175] Eestis on hetkel isikut tõendavate dokumentide seaduse

[172] *Ibid.*
[173] M. Macenaite. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. – New media and society 2017.
[174] A. Thierer. Social Networking and Age Verification: Many Hard Questions; No Easy Solutions. – The Progress & Freedom Foundation 2007.
[175] Roundtable Report. The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society. – Better Internet for Kids, Brussels 2017.

§-i 5 alusel isikutunnistuse omamine kohustuslik alates 15-eluaastast[176], milleks enamasti on ID-kaart. Seega ei saaks ka Eestis kehtestada nõuet, mille abil peaks olema kohustuslik ID-kaardi vahendusel autentimine. Autori hinnangul seaks see liigsed piirangud noortele ning samuti looks kõrged nõudmised tehnilise võimekuse osas, mis on igas vanuses erinev.

Enamikel EL-i riikidel ei ole tegelikult usaldusväärset autentimise süsteemi. Iga liikmesriigi andmekaitseasutused peavad esitama suunised lahenduste ja lähenemisviiside kohta, mis vastavad üldmäärusele. Kahjuks on olemas väga vähe tõendeid selle kohta, kuidas lapsed nõusolekust aru saavad. Mõnest uuringust on selgunud, et lapsed kipuvad otsustama konkreetse olukorra kontekstis oma isikuandmete jagamise osas. Laste otsuste tegemise psühholoogiline kontekst on väga mitmemõõtmeline ja keerukas. Lapsed on eri tingimustes erinevate survete all.[177] Samas tuleb loota, et kõigi asutuste vaheline koostöö nii era- kui ka avalikus sektoris muutub efektiivsemaks ja läbipaistvamaks, et kaitsta ja arendada iga riigi pidevalt laienevat infrastruktuuri. Andmesubjekti ülesanne on harida end küberteemadel ja kaitsta oma andmeid.[178]

Kui analüüsida erinevaid autentimisviise, siis kõige tavalisemad autentimisviisid ulatuvad paroolidest salaküsimusteni. Paroolid on lihtsasti unustatavad ja võivad olla liiga nõrgad, kui neid ei rakendata nõuetekohaselt. Keerulisemad autentimisviisid on näiteks erinevad võtmed, mis on USB-l, PIN-kalkulaatorid. Samuti on olemas kindlamad autentimisviisid nagu sõrmejälgede abil isiku tuvastamine või silma võrkkesta skaneeringuid. Need on usaldusväärsed, kuna tunnused on igaühele ainulaadsed, kuid vanemate tehnoloogiatega on neid raskem kasutada ja rakendada.[179] Kui töödelda näiteks biomeetrilisi andmeid, siis see suurendaks riivet informatsioonilisele enesemääramisõigusele. Sellisel juhul peaks mõtlema, et kas selline riive on antud eesmärgist lähtudes kõige mõistlikum (näiteks töödeldakse eriliigilisi isikuandmeid sotsiaalvõrgustiku konto tegemiseks). Kui isik peaks end autentima biomeetriliste andmete abil, et mõnda sotsiaalvõrgustiku teenust kasutada, siis see oleks autori hinnangul ebaproportsionaalne. Samal ajal ei oleks see ebaproportsionaalne isikuandmete töötlemine, kui oleks vajalik sisse logida e-tervise leheküljele, kuna seal asuvad eriliigilised isikuandmed. Kõige efektiivsemat autentimisviisi on keeruline leida, kuid tuleks koostada analüüse selles osas, millised viisid oleksid vastavas olukorras kõige mõistlikumad ning turvalisemad.

[176] Isikut tõendavate dokumentide seadus[1]. - RT I, 22.03.2017, 3
[177] Roundtable Report (viide 175).
[178] C. Valez. A Glimpse at German Privacy Laws, from a Dark Past to the Strictest Data Protection Laws in Europe (but There is Still a Long Way to Go). – Rutgers Journal of Law and Religion Vol. 18, 2017.
[179] J. Costa. 2FA2P2: A Two Factor Authentication Scheme. – ResearchGate 2017.

Andmekaitse Töörühm on isiku tuvastamise osas näitena välja toonud internetimänguplatvormi soovi tagada, et alaealised kliendid kasutaksid nende teenust ainult oma vanemate või hooldajate nõusolekuga. Töötleja peab järgima neid samme:
1. samm: kasutaja peaks märkima, kas ta on alla 16-aastane. Kui kasutaja väidab, et ta on alla 16-aastane, siis tuleb teine etapp.
2. etapp: teenus teavitab last sellest, et lapsevanem või seaduslik esindaja peab andma lapsele teenuse osutamise nõusoleku või loa töötlemiseks. Kasutajal palutakse avalikustada vanema või eestkostja e-posti aadress.
3. etapp: kontaktid vanemate või seaduslike esindajatega ning nende nõusolek saadetakse e-posti teel töötlemiseks ja võetakse kasutusele mõistlikke meetmeid kinnitamaks, et täiskasvanutel on õigused olemas.
4. etapp: kaebuste korral võtab platvorm kasutaja vanuse kontrollimiseks täiendavaid samme. Kui platvorm vastab teistele nõusoleku nõuetele, võib platvorm järgida üldmääruse artikli 8 lisakriteeriume. Sellisel viisil on andmetöötleja kasutusele võtnud mõistlikud meetmed, mis vastavad üldmääruse nõuetele. Töörühm rõhutab, et töötleja enda otsustada on, mis meetmeid mingites olukordades peaks kasutama. Samuti peab arvestama sellega, et kui kasutaja saavutab mingi aja pärast vastava ea, siis peab kehtiva nõusoleku saama kasutaja enda käest. Seetõttu oleks mõistlik saata kasutajatele meeldetuletusi, et nõusolekud oleksid kehtivad.[180] Üldmääruse rakendamise puhul on mitmeid probleeme. Näiteks pole siiski arusaadav, millisel juhul loetakse andmetöötleja pingutused põhjendatuks. Samuti vajab selgitamist konkreetne nõusolekumehhanism.[181] Isikuandmete töötlejatele on kohati loodud ebaselged reeglid, mis vajaksid täiendavaid tehnilisi täpsustusi kas liikmesriikide järelevalveasutustelt või EL-i üleselt. Samuti on tekkinud suur halduskoormus ettevõtetele ning riive ettevõtete huvidele, kes peavad rangetele tingimustele vastama, et ei tekiks rikkumisi ning ei riivataks isiku informatsioonilist enesemääramist. Näiteks antud sätte puhul võib tekkida riive ka seadusliku esindaja informatsioonilisele enesemääramisõigusele, kui kasutaja ehk laps peab andma oma seadusliku esindaja e-maili isikuandmete töötlejale. Autori hinnangul pole see riive siiski ebaproportsionaalne seadusliku esindaja suhtes, sest lapse isikuandmete turvalisus on antud juhul olulisem.

AKI on öelnud, et võrgulehtede haldajad on kohustatud veebilehel esitama selge ja arusaadava teabe, millist tüüpi küpsiseid nende võrguleht kasutab ja mis eesmärgil. Kui veebilehe kasutaja isikut on võimalik tuvastada, võrguleht vahendab kolmanda osapoole küpsiseid või kui

[180] Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017, page 26.
[181] M. Macenaite, E. Kosta (viide 149).

võrguleht kasutab küpsiseid võrgulehe külastusega mitte seotud eesmärgil, siis tuleb lisaks teavitamisele küsida küpsiste kasutamiseks isiku nõusolekut (nõue kehtib nii avaliku kui ka erasektori asutuste kohta).[182] Huvitaks nüansiks on ka see, et kui teavet kogutakse ainult küpsiste abil, kas vanemate nõusolekut nõutakse ka sellisel juhul? Või on see ainult siis, kui kogutakse teatud liiki teavet? Nõusoleku protsessi tehniline pool on keeruline, kui kasutaja saab teenust ilma kasutajakontot loomata.[183] Tehnilised viisid isikute tuvastamiseks on jäänud ebaselgeks ning küpsiste kasutamisel on tekkinud küsimusi ka seoses lastevanemate nõusoleku temaatikaga.

2.3.3. Lapse informatsiooniline enesemääramisõigus

Oluliseks küsimuseks selles valdkonnas on see, et kuidas parandada vanemate digitaalset kirjaoskust ja kuidas rakendada tõrgeteta vanuse ja nõusoleku sätteid. Vanemad saavad oma laste isikuandmete töötlemise kohta anda nõusoleku, kui nad on digitaalselt võimekad ja neil on nõutavad teadmised teenuse tingimuste ja privaatsusteadete mõistmiseks. Nende väljakutsete ületamiseks on vaja tihedat koostööd ja dialoogi riiklike andmekaitse järelevalveasutuste, ettevõtete ning lastekaitseekspertide vahel.[184] Üldmäärus seab vanematele ja lastele ülemäära suure koormuse keerulises tehnoloogias ja andmepõhises keskkonnas. Efektiivsed andmekaitse piirangud laste andmete kogumisele võivad olla alternatiiviks vanemate nõusolekule. Piirangud võivad olla profiilide koostamisel, turustamisel, õigustatud huvide kasutamisel lapse isikuandmete töötlemiseks [185] Kindlasti on oluline pöörata rohkem tähelepanu lastevanemate harimisele ning õpetamisele seoses erinevate ohtudega, mis võivad tekkida laste isikuandmete töötlemisel.

Samuti on toodud esile, et noored sunnitakse lahkuma mitmetelt platvormidelt, mis on sotsiaalse suhtluse jaoks olulisteks kohtadeks muutunud. Selle globaalse raamistiku arendamiseks on vaja uuringuid, poliitika kujundamist ja sidusrühmade kaasamist. Teadlased, advokaadid, vanurid, poliitikakujundajad ja noored ise peavad tegema koostööd riikidevaheliste strateegiate edendamiseks. Kui seda tehakse efektiivselt, võib selline algatus aidata tagada, et noortel on kasvavale digitaalsele turule võrdne kohtlemine ja väärikus. Ehkki

[182] Andmekaitse Inspektsioon. Kas veebilehel küpsiste kasutamine vajab nõusolekut? – Andmekaitse Inspektsiooni veebileht 12.07.17. Kättesaadav arvutivõrgus: http://www.aki.ee/et/kas-veebilehel-kupsiste-kasutamine-vajab-nousolekut

[183] M. Sloane, K. Alexander. GDPR and the Digital Age of Consent for Online Services. – Tech Law for Everyone 2016. Kättesaadav arvutivõrgus: https://www.scl.org/articles/3582-gdpr-and-the-digital-age-of-consent-for-online-services

[184] T. Bräutigam, S. Miettinen. Data Protection, Privacy and European Regulation in the Digital Age. – Unigrafia OY, Helsinki 2016.

[185] M. Macenaite, E. Kosta (viide 149).

vanemate luba jääb noorte laste jaoks sobivaks kaitseks, võib see siiski piirata teismeliste juurdepääsu teabele, sotsiaalsele suhtlemisele ja osalemisele.[186]

Samamoodi on oluline koolides nii õpetajate kui õpilaste (nt arvutiõpetuse tunnis) hulgas teha rohkem selgitustööd ning tuua praktilisi näiteid, kuidas isikuandmete avaldamine näiteks internetis võib tulevikus kahjustada eraelu puutumatust. Eestis on vanemate/esindajate, laste ja õpetajate teadlikkuse tõstmiseks olemas interaktiivne mäng „Päästa Liisa ID", mis on suunatud kõigi alg- ja põhikooli õpilastele, aga samuti lastevanematele ning õpetajatele.[187] Andmekaitse ja eraelu puutumatuse õpetamine peaks olema õppekava kohustuslik osa, mis peaks hõlmama kõiki õpetajaid, töötajaid ja mis peaks olema integreeritud teistesse teemadesse. Internetis pakutakse laste jaoks suuri võimalusi ja eeliseid. Lastel on võimalik osaleda loometegevuses, luua võrgustikke. Juurdepääs internetile on laste õiguste küsimus. Vanematel on üldmääruse kohaselt võimalik suurel määral piirata laste eneseväljendust ning nad nö ära lõigata erinevatest internetikanalitest.[188]

Reklaamitööstusel on samuti kahtlemata oluline osa erinevate digitaalkeskkondade loomisel, mis on lastele suunatud. Tänapäeva profiilide koostamise keerukus ja ebamäärasus raskendavad lastel otsuste vastuvõtmisel neid hoolikalt kaaluda ja kriitiliselt läbi mõelda. Tegelikult peaks lastele õpetama juba noorena reklaamindusega seotud ohtusid. Osana nende arengu- ja haridusõigustest tuleb varakult õpetada, kuidas reklaamiga toime tulla ka digitaalses keskkonnas.[189] Autori hinnangul on ka oluline integreerida andmekaitse põhimõtteid erinevatesse õppekavadesse ning teadlikkust asjakohastest teemadest suurendada.

Üldmääruse vanemliku nõusoleku sätteid võib pidada lapse privaatsusõiguse seisukohalt suhteliselt probleemseks. Nende sätete aluseks olev lähenemine tekitab pingeid vanemate ja laste vahel. Näiteks ei ole sotsiaalmeedia mitte ainult koht, kus teismelised suhtlevad oma eakaaslastega, vaid ka koht, kuhu nö põgenetakse oma vanemate eest.[190] Lapse privaatsusega on tugevalt seotud õigus enesemääramisele, mis on põhiline psühholoogiline vajadus isikliku kasvu ja heaolu eesmärgil. See jätab alaealisele võimaluse katsetada ning end teostada. Kui

[186] K. C. Montgomery, J. Chester. Data Protection for Youth in the Digital Age. – European Data Protection Law Review 2015.
[187] Andmekaitse Inspektsioon. Laste õigused ja isikuandmete töötlemine 2013.
[188] Roundtable Report (viide 175).
[189] V. Verdoodt, E. Lievens. Targeting Children with Personalised Advertising: How to Reconcile the Best Interests of Children and Advertisers. - Data Protection and Privacy Under Pressure: Transatlantic tensions, EU surveillance, and big data (Maklu 2017).
[190] S. van der Hof. I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World. – Wisconsin International Law Journal 2016.

alaealistel pole võimalik endal otsustada, mis andmeid ja kuidas neid jagada, siis see võib põhjustada probleeme, mis võivad kogu elu jooksul püsida.[191]

Lapsele keskendunud lähenemisviisi vastuvõtmine laste isikuandmete töötlemisel järgib lapse õigusi, kuid keskendub ainult kaitsele. On oluline meeles pidada, et eraelu puutumatuse ja andmekaitsega seotud õigused on laste jaoks olulised. Veelgi enam, kuna üldmääruse keskmes asuvad olulised kaitsemeetmed - näiteks lapsevanemate nõusolek - viivad pigem turvalisuse illusioonini kui tähenduslikule kontrollile, peab lapse õigustele orienteeritud lähenemisviis tunnistama, kui tähtis on rõhutada andmetöötleja vastutust.[192] Autori hinnangul on isegi kõige olulisemal kohal andmetöötlejate vastutuse aspekt, sest eelkõige on nende tagada isikuandmete turvalisus, eesmärgikohasus ning minimaalsus andmete töötlemisel. Kuna alaealiste ning nende vanemate õiguslikud teadmised ja digitaalsed oskused ei pruugi olla nii heal tasemel, siis peaksid ettevõtted rakendama õiglast andmete töötlemist ning vähendama oma tegevusega riivet laste privaatsusele.

Lõpuks on oluline, et lastele pakutakse teadmisi ja vahendeid, mis võimaldavad neil tugevdada oma positsiooni ühiskonnas nii lapsepõlves kui ka täiskasvanueas. Vanematel on kindlasti laste juhtimisel oluline roll, sealhulgas vastutus interneti teadlikkuse tõstmise ees. Sellest hoolimata on uutes tehnoloogiates ka tendents tekitada vanemates ebamõistlikke hirme ja muresid, mis võivad viia vanemate ülemääraste kaitsemeetmeteni ning vähendavad asjatult lapse võimalusi internetikeskkondades osalemiseks. Nõusolek kui vahend andmekaitse kontekstis annab ainult nö kontrolli illusiooni, sest enamik sellest, mida nõusolek peaks reguleerima või saavutama, on tegelikult väljaspool meie kontrolli.[193]

Huvitava näite võib tuua Ameerika Ühendriikidest, kus autori hinnangul riivati õpilase informatsioonilist enesemääramisõigust. Ameerika Ühendriikides leidis aset juhtum, milles õpilane jäi õpetajale koolis vahele teise omasoolisega suudlemisega ja info edastati vanematele ilma õpilase nõusolekuta. See on olukord, kus kohtud peaksid kohaldama rangemat kontrolli ning uurima, kas koolil oli kindel huvi sekkuda isiku eraellu ja kui selline huvi puudus, siis tuleb austada lapse õigusi. Riik peab üleüldiselt tagama, et kasutatakse kõige vähem pealetükkivaid vahendeid alaealise informatsioonilise teabe avalikustamisel.[194] Samas peab

[191] C. F. Hurley. Sharing isn't caring: putting photographs of children on social media under the lens of the GDPR 2016. – Social Science Research Network 2017. Kättesaadav arvutivõrgus: https://ssrn.com/abstract=3109400.
[192] S. van der Hof, E. Lievens. The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. – Communications Law vol 23, 2018.
[193] S. van der Hof (viide 190).
[194] C. M. Cullitan. Please Don't Tell My Mom – A Minor's Right to Informational Privacy. – Journal of Law and Education Vol 40, 2011.

rõhutama, et inimesed kohandavad sageli teemade sisu vastavalt teatud publikule: vähesed räägivad ausalt oma ülemusele oma tööst nii nagu nad oma abikaasale räägivad. Olemas on erinevaid näiteid, kus isikuandmete avalikustamine sotsiaalvõrgustikes on kaasa toonud negatiivse tagajärje: näiteks pole isikuid tööle võetud või on piiratud juurdepääsu ülikoolide andmebaasidele.[195] Siinkohal on tähtis analüüsida juhtumipõhiselt, kas isikuandmete avalikustamine võib rikkuda tulevikus alaealise võimalusi karjäärialaselt, õpingute osas. Kuna tänapäeval on noored aina julgemad ning avalikustavad kohati liiga palju infot enda kohta (erinevaid pilte, videosid), siis see võib tulevikus olla isiku mainele laastav.

Iseseisvuse saavutamise tõttu on oluline, et laps kaasataks teda puudutavate otsuste tegemisse niipea, kui ta on võimeline konkreetse teema üle arutlema ning selle eest ka vastutama. Põhikoolis võiks informatsiooniline enesemääramisõigus olla osa käitumisharjumuste kujundamisest. Näiteks on võimalik õppida igapäevaste kõneluste, teadetetahvli, kooli kodulehe kriitilise jälgimise abil tegema vahet avalikul ja isiklikul informatsioonil, avalikul ruumil ja eraruumil.[196]

Autor on seisukohal, et nõusoleku küsimine lastevanematelt lastele suunatud infoteenuste kasutamisel piirab lapse informatsioonilist enesemääramisõigust. Seda eelkõige seetõttu, et isik ei saa ise otsustada, milliseid andmeid ta saab enda kohta avalikustada. Samuti vähendatakse võimalusi osaleda erinevates sotsiaalvõrgustikes/mängusaitidel. See võib luua olukorra, kus alaealisel pole võimalik arvamust avaldada, suhelda ja arendada oma sotsiaalseid oskusi. Samuti võib tekkida olukord, kus lapsevanem jälgib pidevalt tegevust erinevatel veebisaitidel. Samal ajal olen arvamusel, et nõusoleku küsimisega lapsevanemalt ei teki ebaproportsionaalset riivet lapse informatsioonilisele enesemääramisõigusele, sest sellise konkreetsema kontrollimehhanismi eesmärk on tagada lapse isikuandmete turvalisem töötlemine ja kaitse. See on väga oluline eesmärk, sest lapsed on internetis nõrgemaks osapooleks. Erinevatele spetsiifilistele valdkondadele piirangute kehtestamine oleks ka üheks lahenduseks, kuid pigem on autori hinnangul efektiivsem aktiivsem koostöö lapse ja tema vanemate/seaduslike esindajate vahel. Seega ületab selle eesmärgi tähtsus riive ulatust. Samuti ei ole hetkel loodud ka paremaid kontrollimehhanisme, mis tagaksid sama tulemuse. Lahendusi selle nõude rakendamise osas on erinevaid, kuid autori hinnangul hakkavad erinevad praktikad välja kujunema siis, kui üldmäärust hakatakse kohaldama.

[195] B. Koops, B. Clayton Newell, T. Timan, I. Skorvanek, T. Chokrevski, M. Galic (viide 33).
[196] H. Harro-Loit (viide 42), lk 109, 110.

2.4. Nõusoleku tähtsus senistes kohtulahendites

Kohtuotsuste puhul on oluline märkida, et on mitmeid lahendeid, kus on välja toodud andmesubjekti nõusoleku olemasolu tähtsus, kuid nõusoleku formaalseid ja sisulisi nüansse pole käsitletud. Järgnevalt analüüsib autor relevantseid lahendeid, mis toovad autori arvates esile nõusoleku tähtsuse andmekaitseõiguse olulistes valdkondades. Enamik lahenditest on tehtud viimase viie aasta sees.

Üldkohtu lahend T-343/13, *CN vs Euroopa Parlament* räägib sellest, kuidas 23. septembril 2009 esitas CN, pensionile jäänud endine ametnik, Euroopa Parlamendi (edaspidi „Parlament") veebipõhise vormi kaudu avalduse, milles ta ei olnud rahul toetusega tema puudega pojale ning tööalaste lahendustega, mis olid tekkinud terviseprobleemide tõttu. Parlament leidis, et avaldus on vastuvõetav, kuid ei rahuldanud seda. Seejärel avaldas Parlament oma veebisaidil „teatise liikmetele", milles mainiti hageja nime, tema eluohtlikku haigust ja tema poja tõsist puuet. 2012. aasta aprillis palus taotleja selle teatise väljajätmist Parlamendi veebisaidilt. Parlament väitis, et isikuandmed olid kustutatud alates 8. oktoobrist 2012. Hagejat toetas vaidluses Euroopa Andmekaitseinspektor.[197] Hageja ütles, et tema hinnangul ei ilmnenud dokumendist, milles ta andis nõusoleku oma petitsiooni avaliku käitlemise osas, et ta oleks andnud ühemõttelise nõusoleku tema tervisliku seisundi ja pereliikme olukorra kohta andmete avaldamiseks.[198]

Euroopa Andmekaitseinspektor leidis samuti, et nõusolek peab olema teadlik ja konkreetne ning olema seotud töötlemistegevusega, millest on isikut teavitatud. Veebivormil ei olnud inspektori arvates selgitatud kavandatud töötlemise tagajärgi ning ei olnud mainitud, et delikaatsed andmed tehakse internetis kättesaadavaks.[199] Parlament leidis, et töötlemine oli kookõlas määruse nr 45/2001 nõuetega (määrus üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta), sest hageja oli andnud ühemõttelise nõusoleku oma petitsiooni avalikult käsitleda, teda teavitati nõuetekohaselt ning ta ei kasutanud võimalust petitsiooni anonüümsena töödelda. Samuti oli nõusolek sõnaselge delikaatsete isikuandmete töötlemiseks ja lisas, et määrus ei näe ette võimalust nõusolek tagasi võtta.[200]

[197] EÜKo T-343/13, *CN vs Euroopa Parlament.*
[198] EÜKo T-343/13, *CN vs Euroopa Parlament* p 28.
[199] EÜKo T-343/13, *CN vs Euroopa Parlament* p 41.
[200] EÜKo T-343/13, *CN vs Euroopa Parlament* p-d 36, 37, 39.

Kohus leidis, et hageja esitas vabatahtliku ja teadliku tahteavalduse ning Parlamendi esitatud teabega tähelepanelik tutvumine oleks pidanud mõistlikult võimaldama tal hinnata oma tegevuse tagajärgi. Ühtlasi oli see tahteavaldus konkreetne, kuna Parlament teavitas hagejat asjaolust, et tema kaebus saab olema internetis kättesaadav. Hageja andis ka oma sõnaselge nõusoleku, kui tegi oma aktiivse tegevusega risti lahtrisse. Samuti märgiti, et kohtuotsuses *V vs Parlament* (kaasus, kus hageja ei olnud andnud oma nõusolekut komisjonile, et terviseandmed edastataks parlamendile)[201] polnud olukord sarnane, sest seal käsitleti endise töötaja andmete edastamist Parlamendile ilma selle isiku nõusolekuta.[202]

Autori hinnangul on andmesubjekti jaoks positiivseks muudatuseks nõusoleku tagasivõtmise võimalus, mis varasemalt ei olnud nii levinud. Ka selles lahendis tõi kohus välja, et andmesubjektil polnud võimalik oma nõusolekut tagasi võtta. Eesti on olnud üks vähestest riikidest, kus see õigus ka varasemalt olemas oli (supra 1.2.3.). Autori hinnangul ei ole siiani olnud andmesubjekti isikuandmed nii efektiivselt kaitstud (nõusoleku andmise osas), kui need on üldmääruse järgi. Selle lahendi põhjal saab väita, et tegelikult polnud isik ikkagi end informatsiooniliselt määranud sellisel viisil, nagu ta oleks tahtnud. See võis olla tingitud sellest, et info isikuandmete kasutamise kohta polnud piisavalt täpne või isik ei lugenud erinevaid teavitusi. Paratamatult tekkis olukord, kus andmesubjekt oli kindel, et tema sellisele tegevusele ei andnud oma nõusolekut. Sarnased olukorrad jäävad ilmselt ka uue üldmääruse puhul kehtima, sest paljud andmesubjektid ei ole alati teadlikud, millele nad oma nõusoleku annavad. Samal ajal on üldmäärus olulisi põhimõtteid nõusolekule täpsustanud ja karmistanud, kuid need on autori hinnangul kohati tõlgendatavad. Seega on vajalik probleemide lahendamisele läheneda juhtumipõhiselt.

Euroopa Kohus on teinud lahendi, kus on öeldud, et IP-aadress on isikuandmed ning selle salvestamine ilma isiku nõusolekuta ei ole lubatud. Euroopa Kohus selgitas, et elektrooniliste teabe- ja sideteenuste pakkuja poolt dünaamilise IP-aadressi salvestamine hetkel, kui isik külastab veebilehte, kujutab selle nimetatud sätte tähenduses isikuandmeid. See kehtib sellisel juhul, kui teenusepakkujal on seaduslikud vahendid, mis võimaldavad kõnealust isikut tuvastada tänu täiendavale teabele, mis on selle isiku teenusepakkuja valduses. Direktiivi artikli 7 punktiga f *(„isikuandmeid võib töödelda ainult juhul, kui töötlemine on vajalik vastutava töötleja või andmeid saava kolmanda isiku või kolmandate isikute õigustatud huvide*

[201] EATKo F-46/09, *V vs Parlament* p 138.
[202] EÜKo T-343/13, *CN vs Euroopa Parlament* p-d 74, 75, 92.

elluviimiseks, kui selliseid huve ei kaalu üles artikli 1 lõike 1 kohaselt kaitstavate andmesubjekti põhiõiguse ja -vabadustega seotud huvid") on vastuolus liikmesriigi õigusnormid, mille alusel elektrooniliste teabe- ja sideteenuste pakkuja võib koguda ja kasutada nende teenuste kasutaja isikuandmeid ilma tema nõusolekuta üksnes siis, kui selline kogumine ja kasutamine on vajalik kasutaja poolt elektrooniliste teabe- ja sideteenuste konkreetse kasutuselevõtu võimaldamiseks ja arve esitamiseks.[203] Seetõttu peaks olema küpsiste kasutamise puhul olema tagatud nõusoleku andmise võimalus (juhtudel, kus on võimalik isikut tuvastada). Hetkel on paljudel veebilehekülgedel ainult võimalik nõustuda küpsiste kasutamisega või pole sellist teavitust üldse. Selline isikuandmete töötlemine on problemaatiline ning loodetavasti muutub see olukord üldmääruse kohaldamisel. Samas peab arvesse võtma, et kui dünaamiline IP-aadress muutub, siis ikkagi ei pruugi olla võimekust isiku tuvastamiseks. Üldmäärus loeb IP-aadressi ka isikuandmeteks ehk selle alusel peaks teenusepakkuja suutma isikut tuvastada, kuid tegelikult võib ühe numbrikombinatsiooni taga olla kümneid inimesi ning reaalne võimalus isiku tuvastamiseks puudub (ühel ruuteril on üks väline IP-aadress ja väljastpoolt on näha, et kõikidel arvutitel on sama IP-aadress). Lisaks sellele peaks andmetöötleja isikule tema järelepärimisel andma väljavõtte töödeldud isikuandmest, kuid kuna ettevõtja ei oska seostada arvutit ja isikut, siis ei saa veebilehel küpsise kasutamist isikuga seostada. Andmekaitse Inspektsioon on välja toonud, et isikut ei ole võimalik tuvastada erijuhtudel: kui infoühiskonna teenuse osutajal või avaliku internetiteenuse pakkujal puuduvad seaduslikud vahendid kasutaja tuvastamiseks või infoühiskonna teenuse osutaja või avaliku internetiteenuse pakkuja ei suuda mõistliku jõupingutusega kasutajat kindlaks teha.[204] Autori hinnangul on lahendist tulnud põhimõte tervitatav, kuid peab arvestama, et ka sellistel juhtudel on oluline täiendava teabe olemasolu, mis võimaldab isikuid tuvastada.

Nõusolek on olulisel kohal olnud mitmetes lahendites. Üheks selliseks on *L.H. vs Läti,* kus oli isikule sünnituse ajal tehtud sunniviisiline steriliseerimine ning andmesubjekt pöördus kohtusse. Kohtumenetluse ajal kogus Meditsiiniteenuste Kvaliteedi Kontrolli Inspektsioon 7 aasta jooksul andmeid sünnitusabi ja günekoloogiliste läbivaatuste kohta. Andmesubjekt ei olnud oma nõusolekut sellele andnud. EIK leidis, et niivõrd pika ajaperioodi tagant isikuandmete kogumise eesmärk ei saa olla meditsiinitegevuse kvaliteedi kontrollimine ning asjas oli EIÕK artikkel 8 rikkumine.[205] Selles kohtuotsuses rõhutati terviseandmete kaitsmise ja nõusoleku andmise tähtsust, mis on kindlasti ka üldmääruse kontekstis väga oluline (supra

[203] EKo C-582/14, *Patrick Breyer vs Saksamaa Liitvabariik*.
[204] Andmekaitse Inspektsioon. Juhis organisatsioonidele ja kodukasutajale. IP-aadress ja privaatsus 07.12.2016.
[205] EIKo 52019/07, *L.H. v Läti.*

2.2.). Eriliigiliste isikuandmete töötlemise puhul peab alati hoolikalt analüüsima eesmärgi ning õigusliku aluse olemasolu.

Kohtulahend *Peck vs Ühendkuningriik* selgitab olukorda, kus kohaliku omavalitsuse poolt paigaldatud turvakaameraga tehtud videolõik anti meediale. Isik nimega Geoffrey Dennis Peck oli jäänud turvavideolindile sellega, et käis ringi suure kööginoaga eesmärgiga end ära tappa. Turvavideo kaadritest tehtud pildid jõudsid meediasse (Pecki tuttavad tundsid ta ära). Kohus leidis, et esitatud materjalide avalikustamine ei olnud seotud piisavate kaitsemeetmetega ja kujutas endast ebaproportsionaalset ja põhjendamatut sekkumist hageja eraellu, rikkudes sellega konventsiooni artiklit 8. Materjale poleks tohtinud avalikustada ilma isiku nõusolekuta, sest tegemist polnud avaliku elu tegelasega ning ka muud alust selleks polnud. Kuritegevuse ennetamise eesmärk ja avalikustamise kontekst nõuavad käesolevas asjas erilist tähelepanu ja hoolt. Samuti leiti, et on rikutud konventsiooni artiklit 13 (õigus tõhusale õiguskaitsevahendile) koostoimes artikliga 8, sest hagejal ei olnud tõhusat õiguskaitsevahendit seoses tema õigusega austada tema eraelu.[206] Alati on oluline arvestada erinevaid õiguslikke aluseid, kuid nõusolek võib teatud juhtudel olla kõige kindlam alus isikuandmete töötlemiseks. Eesti isikuandmete kaitse seaduse eelnõu § 4 näeb ette, et isikuandmeid võib töödelda ilma nõusolekuta ajakirjanduslikul eesmärgil, kui on olemas avalik huvi ning see on kooskõlas ajakirjanduseetika põhimõtetega. See ei tohi ülemäära kahjustada andmesubjekti õigusi.[207] Seega on oluline analüüsida juhtumipõhiselt, milline oleks kõige parem lahendus ning milline on õiguslik alus konkreetses olukorras.

Riigikohus on analüüsinud nõusolekut veidi teistsuguses kontekstis, mis polnud seotud kuritegevuse ennetamisega, vaid oli seotud päevakajalise sündmuse kajastamisega. Riigikohtu otsuses nr 3-2-1-152-09 leiti, et kujutise kasutamiseks ilma nõusolekuta polnud täidetud vajalikke eeldusi ning tõdeti, et üldjuhul on keelatud kasutada isiku kujutist juhuslikus seoses päevasündmusega ilma tema nõusolekuta.[208] Sarnase näitena võib tuua EIK otsuse *Société de Conception de Presse et d'Édition vs Prantsusmaa,* mis analüüsis juhtumit, kus isik rööviti ning teda piinati. Perele saadeti fotod piinatud isikust ning meediaväljande kätte sattusid pildid temast. Juhtunud sündmust kajastati ajalehes ja selleks kasutati isikut kujutist, kuigi seda poleks tohtinud teha. Foto oli varasemas kohtuastmes nõutud mustaks teha ning meediaväljaanne otsustas seetõttu kohtusse pöörduda. Kohus leidis, et meediaväljaande väljendusvabadust ei rikutud ning kuna foto avaldati ilma perekonnaliikmete nõusolekuta, siis see näitas sügavat

[206] EIKo 44647/98, *Peck vs Ühendkuningriik.*
[207] Isikuandmete kaitse seaduse eelnõu. 21.03.2018.
[208] RKTKo 3-2-1-152-09, p 13.

lugupidamatust mõrvatud inimese pereliikmete tunnete osas. Ajakirjanik oleks pidanud arvesse võtma fotode mõju eraelule.[209] Selles lahendis rõhutati nõusoleku olulisust biomeetriliste andmete avaldamisel (isikukujutis pildil). Nõusoleku kehtivus on eriti tähtis, kui töödeldakse eriliigilisi isikuandmeid, sest need on tundlikuma iseloomuga ja rangema kaitse all.

[209] EIKo 4683/11, *Société de Conception de Presse et d'Édition vs Prantsusmaa.*

KOKKUVÕTE

Käesoleva magistritöö eesmärk oli käsitleda andmesubjekti isikuandmete töötlemist nõusoleku alusel hetkel kehtiva isikuandmete kaitse seaduse, Euroopa Liidu isikuandmete kaitse üldmääruse, isikuandmete kaitse seaduse eelnõu ja isikuandmete kaitse seaduse eelnõu seletuskirja, AKI juhiste ning asjakohaste teadusartiklite ja Andmekaitse Töörühma suuniste põhjal. Oluline on jõuda järeldustele, kas üldmääruse alusel isikuandmete töötlemine nõusoleku nõuete kohaselt riivab ebaproportsionaalselt lapse informatsioonilist enesemääramisõigust infoühiskonna teenuste kasutamisel, kas andmesubjektide nõusolekule sätestatud nõuded tagavad andmesubjekti informatsioonilise enesemääramisõiguse analüüsitud valdkondades ning kas nõusolekule kohaldatavad nõuded on üldmääruse tähenduses normi rakendamiseks piisavalt õigusselged.

Esimeses peatükis käsitles töö autor andmesubjekti nõusolekule kohaldatavaid regulatsioone, olulisi põhimõtteid ning nõusoleku tõendamiskohustust.

Esimeses alapeatükis analüüsiti nõusoleku olemust nii andmekaitsedirektiivi, üldmääruse, hetkel kehtiva isikuandmete kaitse seaduse, uue isikuandmete kaitse seaduse eelnõu ja selle seletuskirja ning Saksamaa föderaalse andmekaitse seaduse alusel. Analüüsi käigus jõuti järeldusele, et üldmääruse kontekstis on nõusolekule võrreldes andmekaitsedirektiiviga kehtestatud rangemad ja konkreetsemad nõuded, kuid kohati on kehtestatud nõuded liiga üldsõnalised/tõlgendatavad, et neid korrektselt normi rakendamise tasandil kohaldada. Siinkohal on olulisel kohal siseriiklikud õigusaktid, mis saaksid andmekaitsealaseid aspekte täpsustada. Autori hinnangul oleks vajalik isikuandmete kaitse seaduse eelnõus täpsemalt reguleerida nõusolekuga seotud nüansse töösuhtes. Näiteks peaks välja tooma, millistel tingimustel on nõusolek vabatahtlikult antud ning milline on nõusolekule kehtestatav vorminõue, mis olid konkreetselt sätestatud Saksamaa föderaalses andmekaitse seaduses. Samuti oleks vajalik määratleda jälgimisseadmestike kasutamine töösuhtes, mille on esile toonud ka Andmekaitse Inspektsioon.

Teises alapeatükis analüüsis töö autor andmesubjekti nõusolekule kohaldatavaid olulisemaid põhimõtteid, milleks olid informatsiooniline enesemääramisõigus, vabatahtlikkus, ühemõttelisus, eesmärgikohasus, nõusoleku tagasivõtmise võimalus. Töösuhtes ei saa alati põhjendatud isikuandmete töötlemise aluseks nõusolekut lugeda, sest vabatahtlikkuse aspekt võib alluvussuhtes puudu olla ning seetõttu tekib riive andmesubjekti informatsioonilisele

enesemääramisõigusele. Vabatahtlikkuse põhimõtte sisustamine võib teatud juhtudel ettevõttele raskusi valmistada, sest seda võib mitmeti tõlgendada. Seetõttu on ettevõtjatel kohustus analüüsida, milliseid isikuandmeid on võimalik nõusoleku alusel töödelda ning milliste nõusolekule kohalduvate põhimõtetega võib juhtuda, et nõusolek pole kehtivalt antud. Probleemiks on ka see, et mitmed sotsiaalmeedia platvormid küsivad ülemäära palju isikuandmeid, kuid kui andmesubjekt soovib teenust kasutada, siis ei jää tal muud üle, kui anda oma nõusolek. Autori hinnangul peab see olukord muutuma üldmääruse kohaldamisel, sest järgima peab eesmärgikohasuse ja minimaalsuse põhimõtteid. Üldmääruse oluliseks mõtteks on olnud see, et andmesubjektid loeksid isikuandmete töötlemise põhimõtteid, saaksid aru andmete töötlemise eesmärkidest ning annaksid aktiivse tegevusega nõusoleku. Samal ajal ei saa selline viis siiski garanteerida, et andmesubjektile on tagatud informatsiooniline enesemääramisõigus, sest tihti ei loeta asjakohaseid tingimusi või ei süveneta nendesse. Üldmäärus sätestab, et iga eesmärgi puhul on see oluline eraldi välja tuua. Näiteks isikuandmete edastamisel koostööpartneritele, kui see pole teenuse osutamiseks vajalik, on vajalik küsida andmesubjektilt nõusolekut selle eesmärgi kohta. Selline nõue tagab suuremal määral andmesubjektide informatsioonilist enesemääramist, kuid riivab ettevõtjate huve, kelle eesmärgiks on teenust võimalikult palju reklaamida. Autor on seisukohal, et riive ettevõtjate huvidele pole ebaproportsionaalne võrreldes füüsiliste isikute informatsioonilise enesemääramisõiguse teostamisega. Samal ajal peab arvestama, et andmesubjektidel endal on oluline vastutus enda informatsioonilise enesemääramisõiguse sisustamisel.
Nõusoleku tagasivõtmise õigus on ka hetkel kehtivas isikuandmete kaitse seaduses, kuid seda pole mitmetes riikides siiani olnud. Selline õigus loob ebakindlust ettevõtete seas, kuid tagab andmesubjekti informatsioonilist enesemääramist suuremal määral (andmesubjektil on võimalus isikuandmed nö tagasi võtta). Pean kindlasti oluliseks üldmääruse põhimõtet, et nõusoleku tagasivõtmine peab olema sama lihtne kui selle andmine ning leian, et selline õigus on tervitatav.

Kolmandas alapeatükis käsitles autor lühidalt isikuandmete töötleja kohustust andmesubjekti nõusolekut tõendada. Autori arvates tagab kõige kindlamalt kirjalikul viisil nõusoleku võtmine selle kehtivuse. Kirjalikul viisil nõusoleku küsimisel on võimalik korrektselt kõik vajalikud üldmääruse nõuded esile tuua ning ei töödelda ka andmesubjekti biomeetrilisi andmeid, mis juhtuks sellisel juhul, kui nõusolek võetakse ning salvestatakse suulises vormis. Sellisel viisil nõusoleku küsimine ei tekita nii suurt riivet isikuandmete liigi mõttes, sest ei töödeldaks andmesubjekti eriliigilisi isikuandmeid ehk häält. Samuti ei teki andmesubjektile kohustust

anda biomeetrilisi isikuandmeid andmetöötlejale töötlemiseks ning säilitamiseks, mis on autori hinnangul tervitatav informatsioonilise enesemääramisõiguse kontekstis.

Teises peatükis analüüsis töö autor nõusolekuga seotud õiguslikke probleeme üldmääruse, isikuandmete kaitse seaduse eelnõu ning seletuskirja ja varasema kohtupraktika kohaselt.

Esimeses alapeatükis käsitles autor nõusoleku problemaatikat andmete ülekandmisel. Andmete ülekandmise õiguse rakendamisel on määrav roll andmesubjekti nõusolekul. Andmete ülekandmine tähendab seda, et tehnilise võimekuse korral on andmesubjektil õigus taotleda, et tema isikuandmed kantakse näiteks teisele ettevõttele. Õiguse rakendamisel võib tekkida oht andmesubjekti informatsioonilisele enesemääramisele isikutuvastamise seisukohalt (pole hetkel seatud rangeid isikutuvastamise nõudeid), sest võimalik on risk, et isiku enda teadmata saadetakse piiramatus mahus isikuandmeid teisele ettevõttele. Jällegi on see üks tagajärgedest, mida peaks antud õiguse rakendamise puhul arvesse võtma, kuid veebiteenuste kasutamisel on selline võimalus paratamatult alati olemas. Samal ajal on olulisel kohal kolmandate isikute õigused, mis võivad andmete ülekandmise puhul kannatada. Kolmandate isikute puhul on üldmääruse artikli 20 lg 4 alusel välja toodud, et andmete ülekandmine ei tohi kahjustada nende õigusi ja vabadusi. Kolmandale isikule võib informatsioonilise enesemääramise osas riive tekkida, kui ettevõtja arvab, et tal on seaduslik alus isikuandmete ülekandmiseks olemas ning kolmandat isikut ei teavitata sellest ega küsita nõusolekut selle toimingu osas (nt pildi, video ülekandmine ühest sotsiaalvõrgustikust teise). Seetõttu on oluline igas olukorras analüüsida, kas töödeldakse ka teiste isikute isikuandmeid vastavalt üldmääruses sätestatud nõuetele. Andmete ülekandmise õigus suurendab tehnilise võimekuse korral suurel määral vastutava töötleja (nii andmeid edastava kui ka andmeid vastuvõtva töötleja) ehk ettevõtte koormust, sest nõuab kontrollimehhanismi ja ressurssi isikuandmete ülekandmise korral.

Teises alapeatükis leidis autor, et isikuandmete kaitse seaduse eelnõu §-s 6 on teadusuuringu puhul võimalik töödelda isikuandmeid ilma andmesubjekti nõusolekuta, kui need on teadusuuringus pseodunümiseeritud kujul. Samal ajal on pseudonümiseerimise puhul vaja kohaldada üldmääruses sätestatut, sest isikuandmeid on võimalik täiendava teabe korral isikustada/depseudonümiseerida. Seega peaks ka pseudonümiseerimise puhul isikud olema teadlikud, et nende isikuandmeid kasutatakse teadusuuringu jaoks ja selline võimalus on olemas, et andmeid võidakse isikustada. Teadusuuringute puhul on üldmääruse alusel võimalik ka nõusoleku alusel isikuandmeid töödelda. Välja on toodud, et teadusuuringute puhul võivad eesmärgid jääda ebatäpseks ning sellisel juhul oleks vajalik uurimisplaani (töömeetodite ja

uurimisküsimuste osas) esile toomine. Autori hinnangul loob see riski andmesubjekti informatsioonilisele enesemääramisele, sest pole lõpuni selge, mis eesmärkidel ja kuidas isikuandmeid ikkagi töödeldakse. Uurimisplaan ei pruugi anda lõplikku vastust ning eesmärgid võivad teadusuuringu raames muutuda. Samal ajal ei loo uus regulatsioon erandit nõusoleku tagasivõtmise osas ehk teadustööde raames on võimalik samuti nõusolekut tagasi võtta. Siin tuleks kaaluda teadusuuringu läbiviija huve ning andmesubjekti informatsioonilist enesemääramist. Autori hinnangul on teadusuuringutel oluline väärtus ühiskonna arengule ning riive võib vastavalt kindlale olukorrale olla ebaproportsionaalne teadusuuringu läbiviijale, sest seatakse ohtu kogu teadustöö valim, tulemuste kvaliteet ning väärtus.

Kolmandas alapeatükis käsitles autor lapse nõusolekuga seotud küsimusi. Üldmäärus sätestab, et infoteenuste pakkumisel lapsele peab küsima seadusliku esindaja nõusolekut. Lapse vanuse ülempiir on võimalik liikmesriikidel siseriiklikult sätestada (ülempiir peab olema vahemikus 13-16 eluaastat). Isikuandmete kaitse seaduse eelnõus on hetkel lapse vanuse ülempiiriks pandud 13 eluaastat. Autori hinnangul oleks vajalik Eestis korraldada uuringuid, mis selgitaksid välja laste teadmised isikuandmetest ja erinevatest andmekaitsega seotud õigustest. See annaks objektiivse hinnangu vanuse määramisel. Samuti on autor seisukohal, et nõusoleku küsimine lastevanematelt lastele suunatud infoühiskonna teenuste kasutamisel riivab lapse informatsioonilist enesemääramisõigust. Seda eelkõige seetõttu, et lapsel pole endal võimalik otsustada, milliseid andmeid ta tahab avalikustada ning millistel infoühiskonna teenuste platvormidel ta soovib osaleda. Samal ajal on autor arvamusel, et sellise nõude puhul ei teki ebaproportsionaalset riivet lapse informatsioonilisele enesemääramisele, sest selle konkreetse kontrollimehhanismi eesmärk on tagada lapse isikuandmete turvalisem töötlemine ja kaitse. Eriti tähtis on see seetõttu, et lapsed on internetis nõrgemaks pooleks. Erinevatele spetsiifilistele valdkondadele piirangute kehtestamine oleks ka üheks lahenduseks, kuid pigem on autori hinnangul efektiivsem aktiivsem koostöö lapse ja tema vanemate/seaduslike esindajate vahel. Lahendusi selle nõude rakendamise osas on erinevaid, kuid autori hinnangul hakkavad erinevad praktikad välja kujunema siis, kui üldmäärust hakatakse kohaldama. Antud nõudega tekib ka suur halduskoormus ettevõtetele, kes pakuvad infoteenuseid lastele, sest nende vastutuseks jääb isiku tuvastamise küsimus. Küsimused võivad tekkida selles osas, et kuidas seda korrektselt teha ning kuidas tagada nõusoleku kehtivus. Autori hinnangul riivab see ettevõtjate huve. Samal ajal on isegi kõige olulisemal kohal andmetöötlejate vastutuse aspekt, sest eelkõige on nende tagada isikuandmete turvalisus, eesmärgikohasus ning minimaalsus isikuandmete töötlemisel. Kuna alaealiste ning nende vanemate õiguslikud ja digitaalsed teadmised ei pruugi olla nii heal

tasemel, siis peaksid ettevõtted rakendama õiglast andmetöötlust ning vähendama oma tegevusega riivet laste informatsioonilisele enesemääramisõigusele.

Neljandas alapeatükis leidis autor, et Üldkohtu otsuses *CN vs Euroopa Parlament* polnud CN end informatsiooniliselt määranud nii nagu ta oleks tahtnud. See võis olla tingitud ebamäärasest teavitamisest või ei olnud isik teavitusi lugenud piisavalt põhjalikult. Varasemalt ei olnud isikuandmed nii efektiivselt kaitstud (nõusoleku andmise osas), kui need on üldmääruse alusel. Üldkohus tõi ka välja selle, et isikul polnud võimalust nõusolekut tagasi võtta, mis on uus tervitatav õigus üldmääruse kohaselt. Samuti tõi autor töös välja erinevaid kohtulahendeid, mis rõhutasid nõusoleku tähtsust isikuandmete töötlemisel.

Autori hinnangul leidis kinnitust hüpotees, et üldmääruses sätestatud ning magistritöös analüüsitud nõusolekule kohalduvad nõuded ei ole normi rakendamiseks piisavalt õigusselged. Üldmäärus ei anna selgeid suuniseid konkreetsete olukordade osas ning mõned sätted on mitmeti tõlgendatavad, seega oleks vajalik siseriiklikul tasemel konkreetseid nõusoleku aspekte täpsustada (autor tõi eelkõige esile töösuhte näite).
Autori arvates leidis osaliselt kinnitust hüpotees, et üldmääruse nõuded andmetöötluse nõusolekule tekitavad ebaproportsionaalse riive lapse informatsioonilisele enesemääramisele infoühiskonna teenuste kasutamisel. Üldmääruse alusel on olemas riive lapse informatsioonilisele enesemääramisõigusele, kuid see pole ebaproportsionaalne võrreldes laste isikuandmete kaitse eesmärgiga.
Autor hinnangul leidis osaliselt kinnitust hüpotees, et nõusolekule kohalduvad nõuded ei taga andmesubjekti informatsioonilist enesemääramisõigust analüüsitud valdkondades. Oht andmesubjekti informatsioonilisele enesemääramisõigusele nõusoleku alusel töötlemisel võib tekkida teatud olukordades teadusuuringutes ning andmete ülekandmisel.

Magistritöö analüüsist tuli ka esile, et teatud juhtudel tekib nõusoleku nõuete täitmisel koormus ettevõtjatele, kuid see pole autori arvates ebaproportsionaalne võrreldes andmesubjekti informatsioonilise enesemääramisõiguse olulisusega.
Autori hinnangul peaks isikuandmeid andmesubjekti nõusoleku alusel töötlema võimalikult vähe. Ettevõtjad peaksid eelkõige töötlema isikuandmeid teiste üldmääruses sätestatud nõuete alusel. See tagaks andmesubjekti informatsioonilise enesemääramisõiguse suurema kaitse ning tõhusama minimaalsuse põhimõtte täitmise, sest andmesubjektid ei peaks nii palju isikuandmeid andmetöötlejale andma. Samuti ei peaks ettevõtjad liialt analüüsima, kas kõik nõusolekule esitatud nõuded on täidetud ning kas andmesubjekt on nõusoleku kehtivalt andnud.

Isikuandmete töötlemise protsess peab olema läbimõeldud ning selge. Nõusoleku alusel isikuandmete töötlemisel peab kõiki kehtestatud põhimõtteid arvesse võtma ning oluline on töödelda isikuandmeid eesmärgipäraselt, minimaalselt ning läbipaistavalt.

PROCESSING DATA SUBJECT'S PERSONAL DATA ON THE BASIS OF CONSENT

Summary

Data protection is at an important place in today's world, although at times it might seem like data subjects lack control over their personal data. In data protection, consent is one of the most important legal basis' when processing personal data. In this thesis the author will analyse important questions regarding consent according to General Data Protection Regulation (aka GDPR).

On May 25, 2018, the GDPR will be applied in the European Union, which sets more detailed criteria for the processing of personal data. Under Article 6 of the GDPR, the legal basis for the processing of personal data is the consent, the necessity of concluding and fulfilling a contract, fulfilling a legal obligation, protecting the vital interests of natural persons, exercising public authority, a legitimate interest. This thesis analyses the processing of personal data on the basis of consent in the light of the GDPR and existing problems. I have chosen specific areas where the biggest inconsistencies have occurred regarding the processing of personal data on the basis of consent. The relevance and urgency of the topic is illustrated by the number of relevant publications and media coverage.

The purpose of this Master's thesis is to identify the requirements and problems applicable to the consent of the data subject in accordance with the new General Data Protection Regulation and the current regulations.

To achieve the goal, following tasks in the Master's thesis will be set up:

1) highlight the principles / requirements applicable to the consent of the data subject and to analyse them on the basis of different legal regulations and publications;
2) identify problems in the area of data subject's consent and analyse them in accordance with the GDPR, legislation, relevant case law and publications.

Master’s thesis hypotheses are:

1. provisions established under the GDPR and those analysed in this thesis for the protection of personal data on the basis of consent of the data subject do not provide sufficient legal clarity in order to implement the provisions;
2. the requirements for the protection of personal data on the basis of consent under the GDPR disproportionately interfere with a child's informational right of self-determination in the use of information society services;
3. the provisions applicable to processing of personal data on the basis of consent does not ensure the data subject's informational right of self-determination in relevant areas.

The Master’s thesis consists of two chapters, which are divided into sub-chapters. In the first chapter, the author mainly addresses the handling of a data subject's consent according to the Data Protection Directive, the current Personal Data Protection Act, the Personal Data Protection Act Draft, and its explanatory memorandum and the GDPR on the protection of personal data. The analysis of the principles applicable to the consent of the data subject and the burden of proof are also important. In the second chapter, the author analyses the importance of consent in data portability, in scientific research and the use of information society services in the case of a child.

The author has mainly used an analytical method. According to the author of the Master’s thesis, there is little legal literature on the subject of the Master's thesis in Estonia. The author has relied on Estonian and European Union legislation, materials of the European Union institutions, relevant literature as well as the case-law of the Court of Justice of the European Union and rulings of the European Court of Human Rights.

The terms which describe this Master’s thesis are data protection, consent, General Data Protection Regulation and informational right of self-determination.

According to the author, the hypothesis that the provisions for the protection of personal data on the basis of the consent provided by the GDPR and analyzed in the Master's thesis do not provide sufficient legal clarity in order to implement the provisions was confirmed. The GDPR does not provide clear guidance for more nuanced situations, and some provisions are

ambiguous, so it would be necessary to specify some aspects of consent at the national level (the author highlighted the example of an employer-employee relationship).
In the author's opinion, the hypothesis that the provisions in the GDPR concerning consent for processing of data disproportionately interfere with a child's informational self-determination in the use of information society services was partly confirmed. Under the GDPR, there is a infringement on the child's right to self-determination, but this is not disproportionate to the objective of protecting children's personal data.
The author identified that the processing of personal data on the basis of the requirements applicable to consent could not ensure the data subject's informational right of self-determination was partly confirmed. Infringement to the data subject's right to informational self-determination may arise in certain circumstances in scientific research and when exercising the right to data portability. It became clear from the analysis that in certain cases the interests of entrepreneurs are infringed upon, but they are not disproportionate in the author's opinion compared to the importance of the data subject's informational right of self-determination.

In author's opinion, personal data should be processed as little as possible on the basis of consent. Entrepreneurs should, in particular, process personal data on the basis of other requirements laid down in the GDPR. This would ensure greater protection of the data subject's right to self-determination and the principle of data minimization, as data subjects would not have to provide as much personal data to the data processor. Similarly, entrepreneurs wouldn't have to analyse if all the requirements for consent were met and whether the data subject has given the consent validly. It is therefore important to process personal data in a minimal and purposeful way.

KASUTATUD LÜHENDID

AKI	Andmekaitse Inspektsioon
Andmekaitsedirektiiv	24.10.1995 a direktiiv 95/46/EÜ
EIK	Euroopa Inimõiguste Kohus
EL	Euroopa Liit
IKS	isikuandmete kaitse seadus
Üldmäärus	isikuandmete kaitse üldmäärus

KASUTATUD ALLIKATE LOETELU

Kasutatud kirjandus

1. A. Forde. The Conceptual Relationship between Privacy and Data Protection. – Cambridge Law Review 2016.
2. A. Suuberg. The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law. - Tulane Journal of Technology and Intellectual Property 2013.
3. A. A.I. Vranaki. Regulating Social Networking Sites: Facebook, Online Behavioral Advertising, Data Protection Laws and Power. – Rutgers Computer & Technology Law Journal 2017.
4. A. Bussche Freiherr, A. Zeiter. Implementing the EU General Data Protection Regulation: A Business Perspective. – European Data Protection Law Review 2016.
5. A. D. Vanberg, M. Bilal Ünver. The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? – European Journal of Law and Technology 2017.
6. B.-J. Koops, B. Clayton Newell, T. Timan, I. Skorvanek, T. Chokrevski, M. Galic. A Typology of Privacy. – University of Pennsylvania Journal of International Law 2016.
7. C. Valez. A Glimpse at German Privacy Laws, from a Dark Past to the Strictest Data Protection Laws in Europe (but There is Still a Long Way to Go). – Rutgers Journal of Law and Religion Vol. 18, 2017.
8. D. W. Schartum. Intelligible Data Protection Legislation: A Procedural Approach. – Oslo Law Review 2017.
9. D. Krivokapic, J. Adamovic. Impact of General Data Protection Regulation on Children's Rights in Digital Environment. – Belgrade Law Review No. 3, 2016.
10. D. J. Solove. Privacy Self-Management and the Consent Dilemmas. - Harvard Law Review, vol. 126, 2014.
11. E. J. Eberle. The Right to Information Self-Determination. – Utah Law Review 2001.
12. H. Ursic. Legal Barriers and Enablers to Big Data Reuse. – European Data Protection Law Review 2016.
13. I. Graef, M. Husovec, N. Purtova. Data Portability and Data Control. Lessons for an Emerging Concept in EU Law. - Tilburg Law School Legal Studies Research Paper Series No. 22/2017.

14. Isikuandmete kaitse seaduse eelnõu seletuskiri. 06.11.2017. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_en_9.11.17.pdf.
15. Isikuandmete kaitse seaduse eelnõu seletuskiri. 21.03.2018. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_sk_21.03.18.pdf.
16. J. Mišek. Consent to Personal Data Processing – The Panacea or the Dead End? – Masaryk University Journal of Law and Technology 2014.
17. J. M. M. Rumbold. B. Pierscionek. The Effect of the General Data Protection Regulation on Medical Research. – Journal of Medical Internet Research 2017.
18. J. Carr. The position of children and their rights under the GDPR. – The London School of Economics and Political Science. Media Policy Project 2017.
19. J. Rauhofer. Of Men and Mice: Should the EU Data Protection Authorities Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle? – European Data Protection Law Review 2015.
20. K. C. Montgomery, J. Chester. Data Protection for Youth in the Digital Age. – European Data Protection Law Review 2015.
21. L. Edwards. Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. – European Data Protection Law Review 2016.
22. L. Scudiero. Bringing Your Data Everywhere: A Legal Reading of the Right to Portability. – European Data Protection Law Review 2017.
23. M. Maidla. Milline on teaduse tähtsus ja sotsiaal-majanduslik mõju? – Sirp 2017.
24. M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Kirjastus Juura 2011.
25. M. J. Taylor, E. S. Dove, G. Laurie, D. Townend. When can the Child Speak for Herself? The Limits of Parental Consent in Data Protection Law for Health Research. – Medical Law Review Vol. 0, 2017.
26. M. Paez, M. L. Marca, The Internet of Things: Emerging Legal Issues for Businesses. – Northern Kentucky Law Review 2016.
27. M. Rondel. Informatsioonilise enesemääramise õigus ja jälitustegevus. – Juridica X, 2016.
28. M. Mostert, Annelien L Bredenoord, Monique CIH Biesaart and Johannes JM van Delden. Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. – European Journal of Human Genetics 2016.
29. M. Goddard. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. - International Journal of Market Research 2017.
30. M. Macenaite, E. Kosta. Consent for processing children's personal data in the EU: following in US footsteps? – Information and Communication Technology Law 2017.

31. N. Bertels. Scientific research under the GDPR: what will change? - KU Leuven Centre for IT & IP Law 2016.
Arvutivõrgus kättesaadav: https://www.law.kuleuven.be/citip/blog/scientific-research-under-gdpr-what-will-change/
32. P. K. Tupay. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. – Juridica IV, 2016.
33. P. D. Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. – Computer Law and Security Review 2017.
34. P. Schwartz. The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination. – The American Journal of Comparative Law 1989.
35. P. Blume. The Data Subject. – European Data Protection Law Review 2015.
36. P. Swire, Yianni Lagos. Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. – Maryland Law Review 2013.
37. R. Alexy. Põhiõigused Eesti põhiseaduses. - Justiitsministeerium. Põhiseaduse juriidilise ekspertiisi komisjon 1997. Kättesaadav arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/elfinder/article_files/prof_robert_alexy._pohioigused_eesti_pohiseaduses.pdf.
38. S. Kulevska. Humanizing the Digital Age: A Right to Be Forgotten Online? – Faculty of Law. Lund University 2014.
39. S. Montelone. Addressing the Failure of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation. – Syracuse Journal of International Law and Commerce 2015.
40. S. van der Hof. I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World. – Wisconsin International Law Journal 2016.
41. S. Livingstone, J. Carr and J. Byrne. "One in Three: Internet Governance and Children's Rights." - Global Commission on Internet Governance Paper Series 2015.
42. S. Stalla-Bourdillon, A. Knight. - Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. – Wisconsin International Law Journal 2016.
43. S. A.Tovino. The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons. – Seton Hall Law Review 2017.

44. V. Mayer-Schonberger, Y. Padova. Regime change? Enabling big data through Europe's new data protection regulation. – The Columbia Science and Technology Law Review 2016.
45. Ü. Madise jt. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Põhiseaduse kommentaarid. Tallinn: Juura 2012. Kättesaadav arvutivõrgus:http://www.pohiseadus.ee/index.php?sid=1&pt=&p=26#c24.

Kasutatud õigusaktid

46. Elektroonilise side seadus. - RT I, 01.07.2017, 2.
47. Euroopa Liidu põhiõiguste harta. - ELT C 326/02 2012. Kättesaadav arvutivõrgus: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:et: PDF.
48. Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EÜT L281, 23.11.1995. Kättesaadav arvutivõrgus: http://eurlex.europa.eu/legalcontent/et/ALL/?uri=CELEX:31995L0046.
49. Euroopa Parlamendi ja Nõukogu määrus 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679.
50. Euroopa Parlamendi ja Nõukogu määrus, 10.01.2017, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). Kättesaadav arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52017PC0010.
51. Isikuandmete kaitse seadus. – RT I, 06.01.2016, 10.
52. Isikuandmete kaitse seaduse eelnõu. 06.11.2017.
53. Isikuandmete kaitse seaduse eelnõu. 21.03.2018. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_en.21.03.18.pdf.
54. Isikuandmete kaitse seaduse rakendamise seaduse eelnõu. 15.03.2018. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_rs_en.pdf.
55. Isikut tõendavate dokumentide seadus[1]. - RT I, 22.03.2017, 3.

56. The Bundestag. Federal Data Protection Act. Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 30.06.2017. Kättesaadav arvutivõrgus: https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf.

Kasutatud kohtulahendid

57. EATKo F-46/09, *V vs Parlament.*
58. EÜKo T-343/13, *CN vs Euroopa Parlament.*
59. EKo C-582/14, *Patrick Breyer vs Saksamaa Liitvabariik*.
60. EIKo 44647/98, *Peck vs Ühendkuningriik.*
61. EIKo 52019/07, *L.H. vs Läti.*
62. EIKo 4683/11, *Société de Conception de Presse et d'Édition vs Prantsusmaa.*
63. RKTKo 3-2-1-152-09.
64. RKTKo 3-2-1-159-14.
65. RKTKo 3-2-1-153-16.
66. RKKKo 3-1-1-80-97.
67. RKHKo 3-3-1-3-12.

Muud allikad

68. A. Thierer. Social Networking and Age Verification: Many Hard Questions; No Easy Solutions. – The Progress & Freedom Foundation 2007.
69. Andmekaitse Inspektsioon. Andmekaitse Inspektsiooni täiendavad seisukohad uue andmekaitseõiguse kontseptsiooni asjus 22.06.2017.
70. Andmekaitse Inspektsioon. Elektrooniliste kontaktandmete kasutamine otseturustuses 2015.
71. Andmekaitse Inspektsioon. Ettekanne Riigikogule 2003. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/2003.rtf, 21.02.2018.
72. Andmekaitse Inspektsioon. Isikuandmete kaitse seaduse eelnõule arvamuse avaldamine 21.12.2017. Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/eelnoule_arvamuse_avaldamine_-_uus_iks.pdf.
73. Andmekaitse Inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal 2014.

74. Andmekaitse Inspektsioon. Juhis organisatsioonidele ja kodukasutajale. IP-aadress ja privaatsus 07.12.2016.
75. Andmekaitse Inspektsioon. Kas veebilehel küpsiste kasutamine vajab nõusolekut? – Andmekaitse Inspektsiooni veebileht 12.07.17. Kättesaadav arvutivõrgus: http://www.aki.ee/et/kas-veebilehel-kupsiste-kasutamine-vajab-nousolekut
76. Andmekaitse Inspektsioon. Laste õigused ja isikuandmete töötlemine 2013.
77. Andmekaitse Inspektsioon. Mida tähendab andmete ülekandmise õigus? – AKI koduleht, 15.09.2017. Kättesaadav arvutivõrgus: http://www.aki.ee/et/andmekaitse-reform/mida-tahendab-andmete-ulekandmise-oigus
78. Andmekaitse Inspektsioon. Mis on andmekaitsealane mõjuhinnang? – AKI koduleht, 09.10.2017. Kättesaadav arvutivõrgus: http://www.aki.ee/et/andmekaitse-reform/mis-andmekaitsealane-mojuhinnang.
79. Andmekaitse Inspektsioon. Nõusoleku kontrollnimekiri 2017. Kättesaadav arvutivõrgus: http://www.aki.ee/et/andmekaitse-reform/nousoleku-kontrollnimekiri.
80. Andmekaitse Inspektsioon. Telefonikõnede salvestamise lubatavuse juhend 2012.
81. Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 28.11.2017.
82. Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. – European Commission 2013, 02.04.2013 .
83. Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 04.04.2017.
84. Artikli 29 alusel alustatud Andmekaitse Töörühm. Suunised andmete ülekandmise õiguse kohta, 05.04.2017.
85. B. Custers, S. van der Hof, B. Schermer, S. Appleby-Arnold, N. Brockdorff. Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law. – SCRIPTed 2013.
86. B. Marr. Privacy Shield - Is Safe Harbour's Replacement Up To The Job In 2017? – Forbes 2017.
87. B.-J. Koops. The Trouble with European Data Protection Law. – TILT Law and Technology Preprint Publications 2014.
88. C. M. Cullitan. Please Don't Tell My Mom – A Minor's Right to Informational Privacy. – Journal of Law and Education Vol 40, 2011.

89. C. F. Hurley. Sharing isn't caring: putting photographs of children on social media under the lens of the GDPR 2016. – Social Science Research Network 2017. Kättesaadav arvutivõrgus: https://ssrn.com/abstract=3109400.
90. Euroopa Liidu Põhiõiguste Amet. Juurdepääs andmekaitse õiguskaitsevahenditele Euroopa Liidu liikmesriikides. – Euroopa Liidu Põhiõiguste Amet väljaannete talitus 2013.
91. European Commission. Attitudes on Data Protection and Electronic Identity in the European Union. – Special Eurobarometer 359 2011. Kättesaadav arvutivõrgus: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf.
92. European Commission. Commission Staff Working Paper. Executive Summary of the Impact Assessment. – Brussels 2012.
93. European Commission. Data Protection. Report. – Special Eurobarometer 431 2015.
94. European Union Agency for Fundamental Rights. Council of Europe. Handbook on European data protection law 2014.
95. E. Lievens, I. Milkaité. Age of consent in the GDPR: updated mapping of recent national guidance and proposals. – Better Internet for Kids 16.08.2017. Arvutivõrgus kättesaadav: https://biblio.ugent.be/publication/8528973/file/8528974.pdf
96. Facebook. Statement of Rights and Responsibilities 31.01.2018. Kättesaadav arvutivõrgus: https://www.facebook.com/legal/terms/update.
97. G. Maldoff. How GDPR changes the rules for research. – The International Association of Privacy Professionals 2016. Arvutivõrgus kättesaadav: https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/
98. G. Chassang. The impact of the EU general data protection regulation on scientific research. – Ecancermedicalscience 2017.
99. H. Harro-Loit. Informatsiooniline enesemääramine kui üks teabekeskkonnas toimetuleku võtmekontseptsioonidest. – Tartu Ülikooli haridusuuringute ja õppekavaarenduse keskus 2010. Kättesaadav arvutivõrgus: https://dspace.ut.ee/bitstream/handle/10062/40923/Uld_Oppekavad1.pdf?sequence=1.
100. J. Costa. 2FA2P2: A Two Factor Authentication Scheme. – ResearchGate 2017.
101. L. Urquhart, N. Sailaja, D. McAuley. Realising the right to data portability for the domestic Internet of things. – Pers Ubiquit Comput 2017.
102. L. Irwin. How to create GDPR – compliant consent forms. – IT Governance Blog 2017.
103. M. Sloane, K. Alexander. GDPR and the Digital Age of Consent for Online Services. – Tech Law for Everyone 2016. Kättesaadav arvutivõrgus:

https://www.scl.org/articles/3582-gdpr-and-the-digital-age-of-consent-for-online-services

104. M. Macenaite. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. – New media and society 2017.
105. O. Lynskey. Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order. – International and Comparative Law Quarterly 2014.
106. Patsiendiportaal. Patsiendi õigused. Kättesaadav arvutivõrgus: http://www.e-tervis.ee/index.php/et/2012-07-22-09-19-35/patsiendiportaali-voimalused/patsiendi-oigused.
107. P. Luts. 200 000 eestlase sotsiaalmeedia konto paroolid murti lahti. – ERR. 15.12.2017.
108. Riigikontrolli aruanne Riigikogule. Riigi tegevus e-tervise rakendamisel, 17.01.2014.
109. Roundtable Report. The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society. – Better Internet for Kids, Brussels 2017.
110. S. Bodoni. Facebook Scandal a 'Game Changer' in Data Privacy Regulation. – Bloomberg 08.04.2018. Kättesaadav arvutivõrgus: https://www.bloomberg.com/news/articles/2018–04–07/facebook–scandal–a–game–changer–in–data–privacy–regulation?utm_campaign=socialflow–organic&utm_source=facebook&cmpid=socialflow-facebook-business&utm_medium=social&utm_content=business.
111. T. Bräutigam, S. Miettinen. Data Protection, Privacy and European Regulation in the Digital Age. – Unigrafia OY, Helsinki 2016.
112. United Nations Educational, Scientific and Cultural Organization. Global Survey on Internet Privacy and Freedom of Expression. – UNESCO Publishing 2012.
113. V. Verdoodt, E. Lievens. Targeting Children with Personalised Advertising: How to Reconcile the Best Interests of Children and Advertisers. - Data Protection and Privacy Under Pressure: Transatlantic tensions, EU surveillance, and big data (Maklu 2017).

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Mari-Lii Piiskop,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

Andmesubjekti isikuandmete töötlemine nõusoleku alusel,

mille juhendaja on LL.M Mari Männiko ja kaasjuhendaja on dr. iur. Mario Rosentau,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, **23.04.2018**