TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Avaliku õiguse osakond

Sandra Velbri

ISIKUANDMETE KAITSE ÜLDMÄÄRUSEST TULENEV NÕUSOLEKU VAJADUS JA SELLE TINGIMUSED ISIKUANDMETE TÖÖTLEMISEL ÄRIÜHINGUTE POOLT

Magistritöö

Juhendaja: *mag. iur.* Sandra Sillaots

Kaasjuhendaja: prof. Ülle Madise

Tallinn

2018

SISUKORD

SISSEJUHATUS 4

1. NÕUSOLEKU KUJUNEMINE ISIKUANDMETE TÖÖTLEMISE ALUSEKS 9
   1.1. Isikuandmete kaitsmise vajadus 9
   1.2. Nõusoleku nõude kujunemine 11
      1.2.1. Rahvusvahelises õiguses 11
      1.2.2. Euroopa Liidus 13
      1.2.3. Eestis kuni tänaseni 15
      1.2.4. Andmekaitse määruses 19

2. NÕUSOLEKU VAJADUS SÕLTUVALT TEISTEST ISIKUANDMETE TÖÖTLEMISE ALUSTEST ANDMEKAITSE MÄÄRUSES 22
   2.1. Isikuandmete töötlemise üldised alused 22
   2.2. Töötlemine lepingu alusel 24
   2.3. Töötlemine seaduse alusel 25
   2.4. Töötlemine andmesubjekti eluliste huvide kaitseks 26
   2.5. Töötlemine avaliku huvi alusel 27
   2.6. Töötlemine õigustatud huvi alusel 28
   2.7. Töötlemine nõusoleku alusel 30
      2.7.1. Nõusoleku alusel töötlemise üldised alused 30
      2.7.2. Nõusoleku alusel töötlemise erijuhud 32
         2.7.2.1. Infoühiskonna teenuse pakkumine lapsele 32
         2.7.2.2. Eriliigiliste isikuandmete töötlemine 36
         2.7.2.3. Isikuandmete edastamine kolmandale riigile või rahvusvahelisele organisatsioonile, kui sellega pole tagatud piisav kaitse 38
         2.7.2.4. Automatiseeritud otsused 39
         2.7.2.5. Otseturundus 42
      2.7.3. Uues isikuandmete kaitse seaduse eelnõus toodud isikuandmete töötlemise erijuhud 47

3. TINGIMUSED KEHTIVALE NÕUSOLEKULE 50
   3.1. Vabatahtlikkus 50
      3.1.1. Valikuvabadus 50
      3.1.2. Jaotatavuse põhimõte 54
   3.2. Konkreetsus 58
   3.3. Teadlikkus 60

3.3.1. Edastamist vajav teave 60
3.3.2. Teabe edastamise viis 64
3.3.2.1. Teabele esitatavad formaalsed nõuded 64
3.3.2.2. Teabe kajastamine koos nõusolekuga vs privaatsuspoliitikas 66
3.3.2.3. Läbipaistvuse põhimõte teabe edastamisel 70
3.4. Ühemõttelisus 72
3.5. Selgesõnalisus 76
3.6. Tagasivõetavus 79
3.7. Nõusoleku vorm ja tõendamisküsimused 82
3.8. Nõusoleku kehtivus 85
3.8.1. Nõusoleku ajaline kehtivus 85
3.8.2. Enne andmekaitse määrust antud nõusolekute kehtivus 86
KOKKUVÕTE 90
The necessity and conditions of consent from General Data Protection Regulation for processing of personal data by companies. Summary 97
KASUTATUD MATERJALID 102

SISSEJUHATUS

Isikuandmed on muutunud 21. sajandil väga väärtuslikuks, mistõttu neid kutsutakse isegi 21. sajandi kaubaks.[1] Arvutite töödeldud andmete maht kahekordistub iga kahe aastaga.[2] Arenenud on pilvandmetöötlus, mille puhul üksikisikud salvestavad kellegi teise serveris olevatesse programmidesse delikaatseid isikuandmeid, kaotades seega nende üle kontrolli.[3] Internetis toimuvast tegevusest tulenevad ohud eraelu puutumatusele ja isikuandmete kaitsele aina suurenevad.[4]

Nende uute ohtudega silmitsi seismiseks peab arenema ka isikuandmete kaitse regulatsioon. 1995. aastal vastu võetud Euroopa Parlamendi ja nõukogu direktiivis, milles käsitletakse üksikisiku kaitset isikuandmete töötlemisel ja selliste andmete vaba liikumist (edaspidi andmekaitse direktiiv)[5] sätestatud isikuandmete kaitse regulatsiooni eesmärgid ja põhimõtted on Euroopa Komisjoni hinnangul endiselt ajakohased. Kahekümne aasta jooksul on aga tehnoloogia kiire areng ja üleilmastumine tekitanud isikuandmete kaitse valdkonnas uusi probleeme.[6] Seega on vaja andmekaitsereegleid põhjalikult reformida, et tugevdada õigust eraelu puutumatusele internetis.[7]

Andmekaitseõiguse reformi vajadust kinnitab ka asjaolu, et Euroopa Komisjoni 2015. aasta uuringus on leitud, et Euroopa Liidus üksnes 24% üksikisikutest usaldavad veebiärisid (sh otsingumootoreid) oma isikuandmete töötlemisel. Samas on inimeste usaldus tervishoiu ja meditsiiniasutuste poolt isikuandmete töötlemise vastu keskmiselt 74%, mis on kolm korda kõrgem veebiäridest.[8] Seega on andmekaitsereeglite reformimine ning isikuandmete töötlemisel nõuete võimalik rangemaks muutmine põhjendatud, sest uuringu tulemused näitavad, et andmesubjektidel puudub isikuandmete töötlemisel usaldus teatud valdkondade suhtes. Samuti näitab see statistika aktuaalsust analüüsida nõusoleku regulatsiooni just äriühingute suhtes.

---

[1] Martini, in: Paal/Pauly, DSGVO, Art. 25 (1. Auflage 2018), rec. 45.
[2] P. K. Tupay. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. Juridica 2016, IV, lk 227.
[3] Komisjoni teatis Euroopa parlamendile, nõukogule, majandus- ja sotsiaalkomiteele ning regioonide komiteele. Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus, KOM(2010) 609 lõplik. Brüssel: 04.11.2010, lk 2. Kättesaadav: https://ec.europa.eu/health//sites/health/files/data_collection/docs/com_2010_0609_et.pdf.
[4] The European Commission DG Justice, Freedom and Security. Study on the economic benefits of privacy enhancing technologies. London Economics: 2010, p 14. Available: https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf.
[5] P. Carey. Data protection: a practical guide to UK and EU law. Oxford: Oxford University Press 2004, p 3.
[6] Komisjoni teatis Euroopa parlamendile, nõukogule, majandus- ja sotsiaalkomiteele ning regioonide komiteele. Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus, KOM(2010) 609 lõplik. Brüssel: 04.11.2010, lk 2. Kättesaadav: https://ec.europa.eu/health//sites/health/files/data_collection/docs/com_2010_0609_et.pdf.
[7] 2018. a. IKS-i eelnõu-i seletuskiri, lk 2.
[8] European Commission. Special Eurobarometer 431. Data Protection Report. 2015, p 66. Available: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf.

Euroopa Komisjoni uuringus on leitud, et seitse inimest kümnest arvavad, et nende andmeid võidakse kasutada muudel eesmärkidel, kui see, milleks neid koguti. Ainult üks viiendik vastanutest väidab, et isikuandmete edastamisel internetis on nad alati informeeritud andmete kogumise tingimustest ja võimalikest kasutusviisidest.[9]

Vajadus uue instrumendi järele on Euroopa Kohtu arvates tingitud ka asjaolust, et käesoleva ajani ei ole liikmesriigid suutnud viia siseriiklikku õigust täielikult direktiiviga kooskõlla.[10] See on toonud kaasa liikmesriikide andmekaitse regulatsioonide killustatuse, õigusliku ebaselguse ja ebaühtlase rakendamine, mis põhjustavad takistusi ettevõtete tegutsemisele ja suurendavad avaliku sektori administratiivset koormust.[11]

Euroopa Komisjoni initsiatiivil on koostatud Euroopa Parlamendi ja nõukogu määrus „üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta", mis võeti vastu 27. aprillil 2016. Andmekaitse määrusega ei muutu küll põhimõte, et isikuandmete töötlemine võib põhineda andmesubjekti nõusolekul, kuid see täpsustab tingimusi, mida ettevõtted peavad kehtiva nõusoleku saamiseks järgima.

Andmekaitse määrus on tekitanud äriühingute seas palju ärevust, sest määrus toob kaasa nõuete rikkumise korral hiigeltrahvid. Nimelt on tõstetud trahvi ülempiiri – kuni 20 miljonit eurot või kuni 4% ettevõtte üleilmsest käibest, sõltuvalt sellest, kumb on suurem. See on pannud äriühingud üle vaatama kõik isikuandmete töötlemisega seonduvad protsessid, mistõttu turul on suur nõudlus andmekaitsealase koolitamise ning juriidilise abi üle. Ärevusele on aidanud kaasa ka ajalehepealkirjad ja koolitusreklaamid, kes hiigeltrahvidele rõhuvad ning sellega kasumit teenivad.[12]

Andmekaitse Inspektsiooni juht on siiski öelnud, et meie järelevalveasutused ei ole karistusorganid, kelle eesmärk on igale avastatud õiguserikkumisele määrata suur rahatrahv ning teenida riigikassasse raha.[13]

Eelneva tõttu on vaja aga selgitada, kas suureks ärevuseks on põhjust. Selleks tuleb vaadata lähemalt, milliseid nõudeid määrus kaasa toob, käsitledes andmekaitse üldmääruse nõusoleku nõudeid ning võrreldes neid kehtiva regulatsiooniga.

---

[9] European Commission. Special Eurobarometer 431. Data Protection Report. 2015, p 13.
[10] Näiteks vt: EKo 16.10.2012, C-614/10, *Commission* vs Austria.
[11] 2018. a. IKS-i eelnõu seletuskiri, lk 3.
[12] V. Peep. Kas isikuandmete kaitse üldmäärus toob tõesti kaasa hiigeltrahvid? 15.11.2017. http://www.aki.ee/et/uudised/uudiste-arhiiv/kas-isikuandmete-kaitse-uldmaarus-toob-toesti-kaasa-hiigeltrahvid.
[13] *Ibid*.

Käesolev töö keskendub üksnes äriühingutele, jättes seejuures kõrvale nõusoleku vajaduse ja tingimused töösuhtes, töötlemisel avaliku sektori poolt ning füüsiliste isikute vahelise isikuandmete töötlemise. Eelnev ei tähenda, et töös käsitletut ei võiks sobivuse korral neile kohaldada.

Määrusega peavad arvestama nii Eestis registreeritud äriühingud, kui ka need, kes pakuvad Eestis oma teenuseid ja kaupu näiteks e-kaubanduse teel. Lisaks peavad määrusega arvestama need äriühingud, kes alles plaanivad Eestis äritegevust ja kes näiteks sellel eesmärgil uurivad Eestis tarbijate käitumist ehk profileerivad kliente. [14]

On leitud, et andmekaitse määrus toob kaasa rangemad nõuded nõusoleku küsimisele, kui oli seatud andmekaitse direktiiviga.[15] Kuna andmekaitse direktiivist ei võetud Eesti õigusesse nõusoleku definitsiooni 1:1 üle, siis tuleb täpsustada, mida nõusoleku definitsiooni muutmine kaasa toob. Muuhulgas just sellele küsimusele annab vastuse käesolev töö, käsitledes nii nõusoleku vajadust kui ka sellele esinevaid nõudeid uue regulatsiooni alusel ning võrreldes seda kehtiva regulatsiooniga.

Töö on aktuaalne, kuna andmekaitse määrusel on väga laiaulatuslik mõju, mis tähendab, et andmekaitse määrus puudutab kõiki ettevõtted üleeuroopaliselt. Lisaks tagab töö aktuaalsuse ka eelnevalt kirjeldatud probleemid üksikisikute usaldamisel ettevõtete poolt isikuandmete töötlemisel.

Seni on rahvusvahelisel tasandil selgitatud erinevates arvamustes, näiteks 2009. aastal andmekaitse direktiivi artikli 29 alusel loodud töörühm (edaspidi andmekaitse töörühm) andmekaitse määrusest tulenevat nõusoleku vajadust ja nõudeid. Samas puudub võrdlus, mis annaks järeldada, kas ja kuidas muutuvad nõusoleku nõuded seoses andmekaitse määruse jõustumisega varasema Eestis kehtiva isikuandmete kaitse regulatsiooni valguses.

Andmekaitse määruse peatse jõustumise tõttu võetakse määruse nõuded üle ning sellega seoses rakendatakse vajalike meetmeid, et viia siseriiklik õigus määrusega kooskõlla. Seega on käesolev töö kasulik juhis neile, kes vaatavad üle oma töötlemise protsesse ning seovad neid õigusliku alusega või uuendavad nõusoleku vorme, et vastata andmekaitse määruse regulatsioonile.

[14] A. Stadnik, Andmekaitse seadusega kaasnevad suured trahvid on müüt. 10.11.2016. https://www.aripaev.ee/uudised/2016/11/10/andmekaitseseadusega-kaasnevad-suured-trahvid-on-muut.
[15] A. Bussche; P. Voigt. The EU General Data Protection Regulation. A practical Guide. Springer: 2017, p 93.

Käesoleva töö esitamise seisuga on uue isikuandmete kaitse seaduse eelnõu esitatud Vabariigi Valitsuselt Riigikogule. Töös lähtutakse isikuandmete kaitse seaduse eelnõust 21.03.2018 seisuga. Uue isikuandmete kaitse seaduse eelnõu kohaselt jõustub seadus 25. mail 2018[16], millega tunnistatakse seni kehtinud isikuandmete kaitse seadus kehtetuks. Kuna eelnõu pole vastu võetud, võib isikuandmete kaitse seaduse eelnõu muutuda.

Käesoleva töö põhieesmärk on teha kindlaks, millistel juhtudel on ettevõtetel isikuandmete töötlemiseks vaja andmesubjekti nõusolekut. Samuti on töö põhieesmärgiks selgitada, kas andmekaitse määrusest tulenevad nõusoleku nõuded muudavad Eesti õigusruumis ettevõtetele kehtiva nõusoleku saamise raskemaks. Eesmärgi saavutamiseks hinnatakse nõusoleku vajadust ja tingimusi kehtiva isikuandmete kaitse regulatsiooniga võrreldes. Töö eesmärk ei ole andmekaitse määrusest tulenevate nõuete kritiseerimine, vaid töös keskendutakse üksnes määrusega kaasnevatele muutustele.

Kooskõlas püstitatud eesmärgiga on kujunenud töö struktuur. Töö on jaotatud kolme peatükki. Töö esimene osa käsitleb nõusoleku nõude kujunemislugu isikuandmete töötlemise õiguslikuks aluseks. Selles peatükis tutvustatakse õigusakte, millest on tuletatav isikuandmete kaitse ning õigusakte, mis tuginevad nõusolekule isikuandmete töötlemise õigustamiseks. Esimeses peatükis on püstitatud uurimisküsimusena, mis hetkest hakati rääkima nõusoleku alusel isikuandmete töötlemisest, kuidas on nõusoleku mõiste kujunenud ning kuidas on see kajastatud õigusaktides.

Töö teine peatükk annab ülevaate nõusoleku vajaduse juhtudest andmekaitse määruse alusel. Teises peatükis otsitakse vastust küsimusele, millal on andmekaitse määruse alusel vaja nõusolekut küsida ning kuidas seda eristada teistest õiguslikest alustest. Samuti käsitleb töö teine peatükk nõusoleku küsimuse vajaduse muutumist võrreldes seni kehtinud regulatsiooniga.

Töö kolmandas peatükis käsitletakse nõusoleku tingimusi. Kolmandas peatükis on püstitatud uurimisküsimus, millistele tingimustele peab kehtiv nõusolek vastama ning milliseid muutusi toovad uued nõuded kaasa võrreldes kehtiva regulatsiooniga.

Töö esimeses osas on käsitletud ajaloolis-kronoloogilist meetodit. Töö teises ja kolmandas osas saavutatakse uurimisküsimustele vastus süsteemse, kvalitatiivse, analüütilise ja võrdleva meetodi abil. Võrdleva meetodi kasutamise eesmärgiks on anda hinnang, kas andmekaitse määrus toob kaasa rangemad nõuded nõusoleku saamisele, kui need on olnud kehtivas isikuandmete kaitse seaduses.

[16] 2018 a. isikuandmete kaitse seaduse eelnõu § 73.

Töö eesmärkide saavutamiseks on töös olulisemate allikatena läbi töötatud andmekaitse üldmääruse, kehtiv isikuandmete kaitse seadus ning uue isikuandmete kaitse seaduse eelnõu. Lisaks eespool kirjeldatud õigusaktidele on töös allikatena kasutatud andmekaitse töörühma arvamusi ning eesti- ja võõrkeelset õiguskirjandust.

Magistritööd iseloomustavad märksõnad on: andmekaitse, andmetöötlus ja isikuandmed.

1. NÕUSOLEKU KUJUNEMINE ISIKUANDMETE TÖÖTLEMISE ALUSEKS

1.1. Isikuandmete kaitsmise vajadus

Informatsioon ja selle liikumine on olnud läbi aegade ühiskonna erilise tähelepanu all – näiteks on inimesed oma kogemusi edasi kandnud ja neid täiendanud[17] ning õiguski on vajanud informatsiooni oma lähtekohtade selgitamise kui ka teostamise eeldusena.[18] 20. sajandi lõpus leiti, et informatsioonist on kujunenud majandusfaktor, kultuuriväärtus ja põhiseaduslikult kaitstav hüve, kui ka potentsiaalne oht.[19]

Üks osa informatsioonist on isikuandmed. Andmekaitse kui õigusharu ei keskendu mitte andmete kaitsele, vaid kaitseb inimest, keda saab kaitstavate andmetega identifitseerida. Andmed on informatsioon kellegi või millegi kohta. Seega isikuandmete puhul on tegemist informatsiooniga mingi isiku kohta.[20]

Euroopa Parlamendi ja Nõukogu Määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (edaspidi andmekaitse määrus) on isikuandmed igasugune teave tuvastatud või tuvastatava füüsilise isiku ehk andmesubjekti kohta (GDPR art. 4 p. 1). See tähendab, et isikuandmed on näiteks isiku nimi, vanus ja kontaktandmed. Isikuandmed on ka andmed näiteks isiku terviseseisundi, rassilise kuuluvuse ja maailmavaadete kohta. Samuti võivad isikuandmed olla andmed isiku kuulumise kohta ametiühingusse.[21]

Andmekaitse määruse artiklis 4 täpsustatakse veel, et tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.

Isikuandmete kaitse seaduses on isikuandmete definitsioon sarnane andmekaitse määruses tooduga.[22] Isik pole tuvastatav, kui tuvastamine nõuab esitatud andmete töötlemist erimeetmete abil[23] või kui isiku tuvastamisele kulub ebamõistlikult palju aega ja tööjõudu.[24] Seega avab

[17] E. Tikk ja A. Nõmper. Informatsioon ja õigus. Tallinn: Juura 2007, lk 13.
[18] A. F. Westin. Privacy and Freedom. 25 Washington & Lee Law Review 166. New York: Athenum 1968, p 36. Available: https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr.
[19] E.Tikk ja A. Nõmper, lk 13.
[20] M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011, lk 42.
[21] Andmekaitse määruse preambula punkt 71.
[22] IKS § 4 lõike 1 kohaselt on isikuandmed on mis tahes informatsioon tuvastatud või tuvastatava isiku kohta sõltumata sellest, millisel kujul või millises vormis need andmed on.
[23] E. Tikk ja A. Nõmper, lk 80.
[24] Appendix to Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical data, p 27.

andmekaitse määrus isikuandmete mõiste põhjalikumalt kui IKS, samas mõiste sisu ei muutmata.

Isikuandmed jagunevad nö tavalisteks isikuandmeteks ja delikaatseteks isikuandmeteks (IKS § 4). Tavalised isikuandmed on näiteks nimi, isikukood, e-mail. Delikaatsete isikuandmete puhul näeb IKS ette konkreetse loetelu. Delikaatsed isikuandmed on oma loomult tundlikud isikuandmed. Ka andmekaitse määrus eristab tavalistest isikuandmetest delikaatseid isikuandmeid, kuid nimetades neid eriliigilisteks isikuandmeteks. Delikaatsete isikuandmete mõiste avatakse täpsemalt peatükis 2.7.2.2.

Algselt oli isikuandmetel peamiselt moraalne väärtus. Seoses ühiskonna arenguga omandasid isikuandmed üha enam ka majandusliku väärtuse.[25] Isikuandmete töötlemine muutus aktuaalsemaks, kui neid hakkasid töötlema ettevõtted seoses oma majandustegevusega.[26] Tänu isikuandmete töötlemisele on ettevõtetel võimalik teada, kuidas ja mida inimesed ostavad. Ettevõtted saavad seda infot ära kasutada ning teha klientidele pakkumisi vastavalt nende vajadustele. Seega võib olla isikuandmete töötlemise ühe eesmärgiks olla müüa kliendile seda, mida ta vajab ning teiseks, selgitada välja, kuidas seda talle müüa.

Kuna isikuandmete töötlemine osutus majanduslikult kasulikuks, hakkasid ettevõtted isikuandmeid massiliselt koguma. See omakorda tähendas, et neid oli mõistlik töödelda automatiseeritud kujul. Ulatuslikumalt on hakatud isikuandmeid automatiseeritud kujul töötlema viimase aastakümne vältel.[27] Töötlemise ulatust näitab ka see, et arvutite töödeldud andmete maht kahekordistub iga kahe aastaga.[28]

Inimene on alati olnud teadlik oma vajadustest ning vaba otsustama, milliseid vajadusi ja kuidas ta rahuldab. Isikuandmete andmisega arvuti kätte on aga esimest korda inimkonna ajaloo jooksul tekkinud tehniline võimekus tõlgendada suurel hulgas andmeid. Tehniline areng on viinud nii kaugele, et arvuti teab juba täna teatud olukordades inimesest endast paremini, mida isik tahab. Sellega on seotud ka isikuandmete majandusliku väärtuse kasv, kuna ettevõtted soovivad kasulikku informatsiooni müügitegevuseks ära kasutada.[29]

Automatiseeritud töötlus võimaldab isikuandmeid töödelda suuremat majandusliku väärtust andval viisil. Seetõttu on viimase paari aasta jooksul isiku kohta käivad andmed muutunud väga

[25] E.Tikk ja A. Nõmper, lk 13.
[26] Y.N Harari. Homo Deus, A Brief History of Tomorrow. London, 2016. p 428-429.
[27] E.Tikk ja A. Nõmper, lk 20.
[28] P. K. Tupay, lk 227.
[29] Y.N Harari, p 429.

väärtuslikuks ning seda kutsutakse isegi 21. sajandi kaubaks. [30] "The Economist" väljaande kohaselt on maailma kõige väärtuslikum ressurss isikuandmed, mitte õli, kuna isikuandmete kaudu saab teada, kuidas ettevõtted oma klientidega suhtlevad ja kuidas see mõjutab positiivselt kliendikogemusi.[31]

Isikuandmed puudutavad mitmeid isiku põhiõigusi, muuhulgas seondub isikuandmete kaitse isiku era- ja perekonnaelu kaitsega (PS § 26), diskrimineerimise keeluga, õigusega võrdsele kohtlemisele (PS § 12) ning ühinemisvabadusega (PS § 48).

Isikuandmete töötlemise laiaulatuslik mõju isiku põhiõigustele ning samal ajal ettevõtete kasvav huvi isikuandmete (automatiseeritus) töötlemise vastu tõi kaasa senisest suurema vajaduse isikuandmete kaitseks.

Isikuandmete kaitse on võimalik nii moraalsete normidega (näiteks kui ühiskond leiab, et sõbra antud saladust ei tohiks edasi rääkida) aga ka institutsionaalsete normidega (näiteks kirjutada reeglid seadusesse). 21. sajandil omandasid isikuandmed nii suure väärtuse, mis omakorda tõi kaasa nii ulatusliku töötlemise, et tekkis vajadus reguleerida rahvusvahelistes ja siseriiklikes õigusaktides.

1.2. Nõusoleku nõude kujunemine

1.2.1. Rahvusvahelises õiguses

Rahvusvaheline vajadus põhiõiguste (sh privaatsuse) kaitseks tekkis pärast Teist maailmasõda, kui maailmas oli tekkinud üldine vajadus riikidevaheliste suhete korrastamiseks ning inim- ja põhiõiguste rahvusvaheliseks reglementeerimiseks.[32]

Privaatsus on seotud isiku erasfääriga ning eraelu tähendab isiku isikliku elu.[33] Seega õigus privaatsusele tähendab õigust isiklikule elule. Isikliku elu juurde kuuluvad paratamatult ka isiklikud andmed, seega on privaatsusõigusega hõlmatud isikuandmed. Sellest tulenevalt on neid kahte õigust vaja eristada, kuna isikuandmete kaitsest on kujunenud õigus, mis seisab eraldi privaatsusõigusest.[34]

Algselt ei reguleeritud rahvusvahelisel tasandil eraldi isikuandmete kaitset, vaid üldist privaatsusõigust. Esimese sammuna võeti rahvusvahelisel tasandil 10. detsembril 1948. Aastal

[30] Martini, in: Paal/Pauly, DSGVO, Art. 25 (1. Auflage 2018), rec. 45.
[31] The Economist. The world's most valuable resource. 06.05.2017.
[32] M. Männiko, lk 15.
[33] *Ibid*, lk 14.
[34] H. Lammerant; P. Hert. Data protection on the Move – current developments in ICTT and Privacy/DataProtection. Springer 2016, p 179.

vastu Ühinenud Rahvaste Organisatsiooni poolt vastu inimõiguste ülddeklaratsioon, mille artikkel 12 sätestab: "Kellegi isiklikku ja perekonnaellu ei või meelevaldselt vahele segada, kellegi korteri puutumatust, kirjavahetuse saladust või au ja reputatsiooni ei tohi meelevaldselt määrida. Igal inimesel on õigus seaduse kaitsel selliste vahelesegamiste ja rikkumiste eest."[35] Seega sätestati ülddeklaratsiooniga esmakordselt õigus eraelu puutumatusele.

4. novembril 1950. aastal võeti Roomas vastu Euroopa inimõiguste ja põhivabaduste konventsioon. Inimõiguste konventsioonis reguleeris eraelu kaitset artikkel 8, mille kohaselt igaühel on õigus eraelu kaitsele.[36] Hiljem on see artikkel olnud selgeks eeskujuks Eesti Vabariigi põhiseaduse § 26 sõnastamisel.[37]

19. detsembril 1966. aastal võeti vastu ÜRO kodaniku ja poliitiliste õiguste rahvusvaheline pakt[38], mille artikliga 17 anti eraelu puutumatusele järgnev sisu:

„1. Kellegi isiklikku või perekonnaellu ei tohi meelevaldselt või ebaseaduslikult vahele segada, kellegi korteripuutumatusele, kirjavahetuse saladusele, aule ja reputatsioonile ei tohi meelevaldselt või ebaseaduslikult kallale kippuda.

2. Igal inimesel on õigus seaduse kaitsele selliste vahelesegamiste ja kallalekippumiste eest."

Eesti ratifitseeris lepingu 1991. aasta 21. oktoobril. Eelnevast nähtub, et rahvusvaheline kaitse privaatsusele on erinevates instrumentides käsitletud sisult üsna sarnaselt.

Kui varem vastuvõetud õigusaktidest nähtuvad eelkõige privaatsuse ja infovabaduse üldised piirid, siis alates 1980. aastate algusest on kehtestatud mitmeid eraldi teabe käibe reguleerimist käsitlevaid instrumente.

Esmakordselt anti privaatsusõiguse põhimõtetele rahvusvahelisel tasandil täpsem sisu 1980. aastal, kui Majandusliku Koostöö ja Arengu Organisatsioon (edaspidi OECD juhend) andis välja juhendi eraelu kaitsest ja piiriülesest isikuandmete kaitsest. Juhendi peamine eesmärk oli kokku leppida OECD liikmesriikidega andmekaitsealased põhimõtted ning toetada ja harmoniseerida põhimõtetega riikide siseriiklikku õigust ning kui siseriiklik õigus andmekaitse valdkonnas puudus, panna alus siseriikliku regulatsiooni loomisele.[39] OECD juhendi artikli 1

[35] ÜRO inimõiguste ülddeklaratsioon A/RES/217, 10.12.1948.
[36] Euroopa inimõiguste ja põhivabaduste konventsioon, RT II 1996, 11, 34. Vastu võetud 4.11.1050, Eestis jõustunud 16.04.1996.
[37] K. Jaanimägi, L. Oja. Põhiseaduse § 26 kommentaar, komm 2. – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017.
[38] Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. Kättesaadav: https://www.riigiteataja.ee/akt/23982. RT II 1994, 10,11.
[39] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD 1980. Available:

punktis b defineeriti isikuandmete mõiste, mis tähendab andmeid, mis on üksikisiku suhtes tuvastatud või tuvastatavad (OECD juhendi artikkel 1 punkt b).

Samuti tuleneb OECD juhendist esmakordselt põhimõte, mille kohaselt isikuandmete töötlemiseks on vajalik andmesubjekti nõusolek. OECD juhendi artiklist 7 tuleneb põhimõte, mille kohaselt isikuandmete kogumisel peaksid olema piirangud ja selliseid andmeid tuleks saada seaduslike ja õiglaste vahendite abil ning vajaduse korral andmesubjekti teadmiste või nõusolekuga. Artikkel 10 lisab, et isikuandmed on lubatud avalikustada, kättesaadavaks teha või muul viisil kasutada otstarbel, mille eesmärki poldud varasemalt andmesubjektile selgitatud, välja arvatud andmesubjekti nõusolekul või kui selleks tuleneb alus seadusest. OECD juhendiga seatakse nõusolek siiski isikuandmete töötlemise eeltingimuseks.[40]

1. oktoobri 1985 Euroopa Nõukogu konventsiooni isikute kaitse kohta isikuandmete automaatsel töötlemisel tuleb artikkel 5 punkti a kohaselt automatiseeritult töödeldavad isikuandmed hankida ja töödelda ausal ning seaduslikul teel.[41] Kõnealuses konventsioonis ei nähtud ette nõusolekut isikuandmete töötlemise üldise alusena, vaid üksnes asutuse poolt välismaal elava andmesubjekti nimel abitaotluse esitamiseks (konventsiooni artikkel 15 p 3).

Kuigi Euroopas oli juba mõnedes seitsmekümnendates aastatel vastuvõetud siseriiklikes andmekaitset ja eraelu puutumatust käsitlevates seadustes ette nähtud isikuandmete töötlemise õiguslik alus, ei kajastatud seda Euroopa Nõukogu konventsioonis. Euroopa Nõukogu konventsioon oli seni ainus isikuandmete kaitse küsimustele pühendatud rahvusvaheline siduv instrument.[42]

Seega hakati andmekaitset eristama üldisest privaatsusõigusest alates 1980. aastatest. Algselt olid määratletud andmekaitse alused üldised, kuid alates OECD juhendist saab rääkida vajadusest töödelda just andmesubjekti nõusolekul. Siiski ei antud OECD juhendiga nõusolekule veel definitsiooni.

1.2.2. Euroopa Liidus

Euroopa Ühenduses tekkis vajadus ühtlustada ja harmoniseerida liikmesriikide vahel isikuandmete töötlemisega seonduvaid õigusakte ning selleks võeti 1995. aastal vastu andmekaitse direktiiv, milles käsitletakse üksikisiku kaitset isikuandmete töötlemisel ja selliste

---

http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[40] Lee A. Bygrace. Data Privacy Law. An International Perspctive. Oxford University Press, 2014, p 160.

[41] 1. oktoobri 1985 Euroopa Nõukogu konventsioon üksikisikute kaitse kohta isikuandmete automaatsel töötlemisel. Strasbourg, 28. jaanuar 1981 aga Eestis jõustus 01.03.2002.

[42] E. Tikk ja A. Nõmper, lk 67.

andmete vaba liikumist. Tegemist on Euroopa riikide isikuandmete kaitse õiguse arengu seisukohalt seni olulisima alusdokumendiga, mis määratles ära isikuandmete kaitse põhimõtted ja eesmärgid, samuti defineeris kesksed mõisted ja määratles töötlemise õiguslikud alused. Seega reguleeris andmekaitse direktiiv Euroopa Liidus esmakordselt andmekaitse valdkonda. Direktiiv kinnitas varasemad andmetöötluse põhimõtted ning lisaks täpsustas õiguslikud alused, mille alusel töötlemine on seaduslik.[43] Direktiivi koostamisel oli aluseks Euroopa Nõukogu konventsioon ja OECD juhend, kuna neis kajastusid isikuandmete töötlemise põhimõtted.[44]

Üheks seadusliku töötlemise aluseks Euroopa Liidu tasandil nähti andmekaitse direktiivis ette töötlemine nõusoleku alusel.[45] Nimelt nägi andmekaitse direktiiv ette õiguslike alustena artikli 7 kohaselt nõusoleku, lepingu või taotluse, seaduse, eluliste huvide kaitse, avalikes huvides oleva ülesande täitmise või õigustatud huvi. Andmesubjekti nõusolekut on defineeritud artiklis 2 punktis ka kui iga vabatahtlik, konkreetne ja teadlik tahteavaldus, millega andmesubjekt annab nõusoleku töödelda tema kohta käivaid andmeid. Lisaks tulenes artikli 7 punktist a, et nõusolek tuleb anda ühemõtteliselt.

Andmekaitse direktiivi täiendab Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (edaspidi e-privaatsuse direktiiv). E-privaatsuse direktiiv oli vajalik, et kohandada eraelu puutumatuse kaitset seoses elektrooniliste sideteenuste turu ja tehnoloogia arenguga [46] ning sellega ühtlustatakse siseriiklike akte isikuandmete kaitse tagamiseks elektroonilise side sektoris ja vaba liikumise tagamiseks Euroopa Liidus.[47]

Vajadusega sõnastada Euroopa Liidus põhilised inimõigused, kuulutati 7. detsembril 2000 aastal Nice'is välja Euroopa Liidu põhiõiguste harta.[48] Harta artikli 8 punktist 1 tulenes, et igaühel on õigus oma isikuandmete kaitsele. Punkt 2 sätestas, et selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Lisaks, et igaühel on õigus tema kogutud andmetega tutvuda ja nõuda nende parandamist.

[43] M. Männiko, lk 74.
[44] E.Tikk ja A. Nõmper, lk 67.
[45] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent. WP 187. Brussels: 2011. Available: http://ec.europa.eu/newsroom/article29/news-overview.cfm, p 5.
[46] Andmekaitse määruse preambula punkt 4.
[47] M. Männiko, lk 78.
[48] Fundamental Rights Agency, European Commission. Handbook on European Data Protection law. Luxemburg: Publications office of the European Union, 2014, p 20. Available: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

Nõusoleku roll oli selgesõnaliselt tunnustatud Euroopa Liidu institutsiooni poolt alla kirjutatud ELi põhiõiguste hartas isikuandmete kaitset puudutavas osas.[49]Seetõttu tunnistati nõusoleku alusel andmete töötlemine isikuandmete kaitse põhiõiguse oluliseks aspektiks.[50] See tähendab, et nõusolek isikuandmete töötlemise alusena on mänginud EL-i ajaloos andmekaitse- ja privaatsusõiguse kujundamisel olulist rolli.

1.2.3. Eestis kuni tänaseni

Isikuandmete kaitse alus tulenes Eesti õiguses õigusaktide tasandil esmalt 1992. aasta põhiseadusest. Põhiseadusest ei tulene isikuandmete kaitse sõnaselgelt, vaid seda saab sarnaselt rahvusvahelise õiguse instrumentidega tuletada põhiõigusest eraelu puutumatusele (PS § 26).[51] Eraelu puutumatusega on hõlmatud informatsioonilise enesemääramise õigus. [52] Informatsioonilise enesemääratlemise õigus seondub isiku kohta käiva informatsiooniga[53] ning tähendab igaühe õigust ise otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse. Seetõttu on eraelu kaitse üheks oluliseks valdkonnaks isikuandmete kaitse.[54] Tänapäeva informatsioonilise enesemääramisõiguse kontseptsiooni üks oluline seisukoht on kontroll isikuandmete üle, mis väljendub andmesubjektilt nõusoleku küsimises.[55]

Eestis reguleerib isikuandmete kaitset täpsemalt alates 1996. aastal isikuandmete kaitse seadus. [56] Seaduse koostamise vajadus tekkis seoses infotehnoloogiavahendite arengu ja levikuga. Seaduse koostamisel lähtuti Euroopa Nõukogu 1. oktoobri 1985.a. konventsioonist isikute kaitseks automatiseeritud andmetöötluse eest, mis puudutab isiklikku laadi andmeid, Euroopa Ühenduse Nõukogu komisjoni 15. oktoobri 1992. a. isikuandmete kaitse alastest soovitustest, Saksa Liitvabariigi ja liidumaade vastavatest seadustest ja teiste Euroopa riikide vastavatest seadustest (Soome, Taani, Rootsi).[57] Lisaks võeti aluseks ka andmekaitse direktiivi

[49] EL põhiõiguste harta artikkel 8 lõige 2 esimene lause sätestab: Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel.
[50] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 5.
[51] K. Jaanimägi, L. Oja. Põhiseaduse § 26 kommentaar, komm 1. – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017.
[52] E. Tikk ja A. Nõmper, lk 47.
[53] *Ibid*, lk 77.
[54] K. Jaanimägi, L. Oja. Põhiseaduse § 26 kommentaar, komm 24. – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017.
[55] E. Tikk ja A. Nõmper, lk 37.
[56] Isikuandmete kaitse seadus. - RT I 1996, 48, 944.
[57] Seletuskiri isikuandmete kaitse seaduse eelnõu juurde. 1995, lk 1.

eelnõu.[58] Tegemist oli Eestis esimese õigusaktiga, milles reguleeriti isikuandmete kaitset tervikuna ning käsitleti esmakordselt nõusolekut töötlemise alusena.

1996. a. IKS-i § 8 lõike 1 kohaselt oli isikuandmete töötlemise õiguslikuks alusteks leping, elu, tervise või vabaduse kaitse, seadus ja välisleping, avalik huvi, üldine huvi või vastutava töötleja õigustatud huvi. Lisaks on isikuandmete kaitse tagatud 1996.a. IKS-i § 3 lõike 2 punkti 1 kohaselt ka isiku õigusega anda oma isikuandmete töötlemiseks nõusolek. Isiku nõusolek 1996. aasta IKS-I § 10 lõike 1 järgi on selgelt väljendatud tahteavaldus, millega isik lubab oma isikuandmete töötlemist pärast seda, kui teda on teavitatud isikuandmete töötlemise eesmärgist ja õiguslikust alusest; isikuandmete koosseisust ja allikast; kolmandatest isikutest või nende kategooriatest, kellele isikuandmete üleandmine on lubatud; üldiseks kasutamiseks antavate isikuandmete loetelust; vastutava töötleja või tema esindaja nimest ja aadressist. Seega ühendas nõusoleku definitsioon endaga ka teavet, mille pidi andmesubjektile edastama. 1996. a. IKS § 10 lõike 2 järgi pidi kehtiv nõusolek olema seotud konkreetse töötlemise juhuga, antud vabatahtlikult ja võis olla isiku poolt igal ajal tagasi võetud. Nõusoleku tagasivõtmine ei oma tagasiulatuvat jõudu (1996. a. IKS § 10 lg 2). Seadusest tulenevalt nõusolekule kohustuslikku vorminõuet ette ei nähtud.

Isikuandmete kaitse seadust muudeti 1. mail 2004 aastal seoses Eesti liitumisega Euroopa Liiduga, mistõttu pidi Eesti tagama isikuandmete kaitse vastavuse 1995. aastal jõustunud andmekaitse direktiivi nõuetega.[59] Kuna direktiiv oli aluseks juba esimese IKS-i koostamisel, ei muudetud 2004. aastal põhimõtet, et isikuandmete töötlemine on lubatud üksnes juhul, kui andmesubjekt on andnud selleks nõusoleku (2004. a. IKS § 11 lg 1), sest selline õiguslik alus tulenes juba seni kehtinud regulatsioonist. Võrreldes eelmise IKS-i regulatsiooniga, on 2004. aasta IKS-ist jäetud välja isikuandmete töötlemise õigusliku alusena õigustatud huvi.

2004. aastal ei muutunud nõusoleku definitsioon oluliselt. Siiski hakati eristama selgelt nõusoleku definitsiooni ning teavet, mida vaja nõusoleku andmiseks andmesubjektile edastada. Nõusoleku definitsioonist tulenes endiselt, et nõusolek on andmesubjekti teadlik tahteavaldus (2004 a. IKS § 12 lg 1). Teiseks loodi volitatud töötlejale uusi kohustusi, millest ta peab enne nõusoleku andmist andmesubjekti teavitama. Viide subjekti õigusele võtta nõusolek igal ajal tagasi oli ka esimeses IKS-is reguleeritud, kuid 2004ndal aastal lisati vastutavale töötlejale kohustus enne nõusoleku küsimist teavitada juhtudest, millal andmesubjektil on õigus nõuda

[58] Isikuandmete kaitse seaduse seletuskiri. 2004, lk 1. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/fda65853-f05c-3b4e-ad4f-27f017828fcd/Isikuandmete%20kaitse%20seadus, lk 1.
[59] *Ibid*.

isikuandmete töötlemise lõpetamist ning isikuandmete parandamist, sulgemist, kustutamist ja teavitada, millal andmesubjektil on õigus saada juurdepääs tema kohta töödeldavatele isikuandmetele (2004. a. IKS § 12 lg 2 p-d 4 ja 5). Lisaks täiendavatele kohustustele vastutavale töötlejale, tuli IKS-iga sama teavituskohustus ka volitatud töötlejale (2004 a. IKS § 12 lõige 2).

2004. aasta IKS-iga seati esimest korda nõusolekule kehtivusaeg. 2004. a. IKS § 12 lõike 3 kohaselt kehtis nõusolek andmesubjekti eluajal ning 30 aastat pärast andmesubjekti surma, kui andmesubjekt ei ole otsustanud teisiti. Pärast andmesubjekti surma on andmesubjekti isikuandmete (va nimi, sugu, sünni- ja surmaaeg ja surmafakt) töötlemine lubatud andmesubjekti seadusliku esindaja, abikaasa, vanema, lapse, lapselapse, venna või õe kirjalikul nõusolekul, v.a. juhul, kui isikuandmete töötlemiseks nõusolekut ei ole vaja (2004 a. IKS § 13 lg-d 1 ja 2).

Järgmine muudatus 2004. a IKS-is seondub nõusoleku regulatsiooni eeldusega, et vaidluse korral ei ole andmesubjekt oma isikuandmete töötlemiseks nõusolekut andnud (2004 a. IKS § 12 lg 5).[60] Seega peab vastutav töötleja arvestama, et vaidluse korral on tema kohustuseks tõendada, et andmesubjekt on nõusoleku andnud.[61]

Nõusoleku regulatsiooni osas lisati viide tsiviilseadustiku üldosa seaduse (edaspidi TsÜS) tahteavalduse sätetele (2004 a. IKS § 12 lg 4 ls 3). TsÜS-i kohaselt saab teadliku ja selge tahteavalduse iseseisvalt anda üksnes isik, kel on täielik teovõime. Piiratud teovõimega isiku puhul peab nõusoleku andma isiku seaduslik esindaja või annab piiratud teovõimega isikule nõusoleku andmiseks oma nõusoleku või selle hiljem heaks kiitma.

2008. aastal jõustus täna kehtiv isikuandmete kaitse seadus.[62] Isikuandmete kaitse seaduses on üldjoontes säilitatud eelmise kehtiva seaduse nõusoleku regulatsioon. Võrreldes eelmise IKS-i regulatsiooniga, on 2008. aasta IKS-is toodud isikuandmete töötlemise õigusliku alusena taas õigustatud huvi, lubades sellele tugineda ainult juhul, kui see on vajalik kolmandal isikul seoses krediidivõimelisuse hindamisega (2008 a. IKS § 11 lg 6). Muuhulgas on töötlemise üheks õiguslikuks aluseks endiselt nõusolek (2008 a. IKS § 10). Seega on isikuandmete töötlemine nõusoleku alusel Eestis alati olnud läbivalt isikuandmete kaitse seaduse osa. Uue regulatsiooniga täpsustati nõusoleku mõistet ning IKS § 12 lõike 1 alusel on nõusolek andmesubjekti tahteavaldus, millega ta lubab oma isikuandmeid töödelda, mis kehtib üksnes juhul, kui see tugineb andmesubjekti vabal tahtel.

[60] Isikuandmete kaitse seadus. - RT 2003, 26, 158.
[61] Isikuandmete kaitse seaduse seletuskiri. 2004, lk 25.
[62] Isikuandmete kaitse seadus - RT I 2007, 24, 127… RT I, 06.01.2016, 10.

2008. a kehtima hakanud IKS-is muudeti isikuandmete mõistet. Loobutud on Eesti õigusesse avaliku teabe seadusega kasutusele võetud isikuandmete kolmikjaotusest (isikuandmed, eraelulised isikuandmed ja delikaatsed isikuandmed). Edaspidi eristatakse kahte jaotust ehk isikuandmeid ja delikaatseid isikuandmeid.

Samuti on muudetud nõusoleku definitsiooni. Lisaks juba varasemalt sätestatule, et nõusolek on andmesubjekti tahteavaldus, millega ta lubab oma isikuandmeid töödelda, on lisatud, et see kehtib üksnes juhul, kui see tugineb andmesubjekti vabal tahtel (2008. a IKS § 12 lg 1 ls 1). Lisaks võib 2008. a. IKS-i kohaselt andmesubjekti nõusolek tema isikuandmete töötlemiseks olla osaline ja tingimuslik (2008 a. IKS § 12 lg 1). Osaline nõusolek tähendab, et andmesubjekt võib anda nõusoleku oma andmete töötlemiseks üksnes ühel eesmärgil mitmest või lubada andmeid üle anda vaid teatud isikutele või nende kategooriatele. Tingimuslik nõusolek tähendab, et andmesubjekt võib anda nõusoleku oma isikuandmete töötlemiseks näiteks ajalise piiranguga või tingimusel, et andmeid ei anta üle kolmandatele isikutele.[63]

Kui varasemalt nõusolekule vorminõue seaduses puudus, siis alates 2008. aastast näeb seadus ette vähemalt kirjalikku taasesitamist võimaldava vormi, välja arvatud juhul, kui vorminõude järgmine ei ole andmetöötluse erilise viisi tõttu võimalik (2008. a. IKS § 12 lg 4 ls 1). Seega jääb andmetöötlejale õigus igal üksikjuhtumil otsustada sobiva vormivaliku üle. Kui nõusolek isikuandmete töötlemiseks on komplekse tehingu üks osa, peab isikuandmete töötlemise nõusolek olema muude tehingu tingimuste hulgast selgesti eristatav (2008 a. IKS § 12 lg 4 ls 2). Näiteks sõlmides kindlustuslepingut, on isikuandmete töötlemist käsitletav blokk alati selgelt eristatav muudest lepingutingimustest. Eesmärk on isiku jaoks eristada, et lisaks võlaõiguslikele tingimustele, mida talle on juba selgitatud ja nõustunud, kirjutab ta muuhulgas alla ka isikuandmete töötlemise nõusolekule.[64]

2008. a. IKS-i kohaselt peab vorm peaks siiski olema selline, et see võimaldaks tuvastada, et nõusolek on selge ja teadlik.[65] Vaikimist või tegevusetust nõusolekuks ei loeta (2008 a. IKS § 12 lg 3). Samuti ei ole lubatud panna andmesubjektile kohustust sooritada mingi täiendav toiming selleks, et vältida isikuandmete töötlemist. Seetõttu pole õiguspärane isikuandmete töötlemine juhul, kui andmesubjekti teavitatakse enne töötlemise alustamist elektroonilise teatega töötlemise algusest ning kui andesubjekt töötlemisega nõus ei ole, siis peab ta sellest mingi aja jooksul teada andma. [66]

[63] Isikuandmete kaitse seaduse seletuskiri. 1026 SE. Justiitsministeerium, lk 13.
[64] *Ibid*.
[65] *Ibid*.
[66] *Ibid.*

Uuena on 2008. aasta IKS-is välja toodud andmesubjekti õigus igal ajal keelata teda käsitlevate andmete töötlemine tarbijaharjumuste uurimiseks või otseturustuseks ja andmete üleandmine kolmandatele isikutele, kes soovivad neid kasutada tarbijaharjumuste uurimiseks või otseturustuseks (2008. a. IKS § 12 lg 5). Kuigi otseturustamine on hõlmatud üldise õigusega anda nõusolek isikuandmete töötlemiseks konkreetsel eesmärgil ning seda võib igal ajal tagasi võtta, siis direktiiv on pannud töötlejatele täiendava teavitamiskohustuse. Nii tarbimisharjumuste uurimine kui ka otseturustamine on üks töötlemise liik. Töötlemise eesmärgid tuleb nõusoleku küsimise ajal andmesubjektile teatavaks teha. Seega võib andmesubjekt nõusoleku andmisel keelata andmete töötlemine otseturustamise või tarbimisharjumuste uurimise eesmärgil. [67]

Nõusolek on olnud Eesti õiguses seega alati isikuandmete töötlemisel üheks õiguslikuks aluseks. Aja jooksul on nõusolekule lisandunud täiendavaid nõudeid, mida nõusoleku võtmisel peab järgima.

Täna kehtiva regulatsiooni alusel on andmesubjekti nõusolek vabatahtlik ja informeeritud tahteavaldus, mis peab olema esitatud kirjalikku taasesitamist võimaldavas vormis. Millised nõuded esitab nõusolekule andmekaitse määruses, kirjeldatakse järgmises alapeatükis.

1.2.4. Andmekaitse määruses

Euroopa Komisjon on märkinud, et andmekaitsereegleid on vaja põhjalikult reformida, et tugevdada õigust eraelu puutumatusele internetis. Reformi eesmärgiks on ajakohastada kehtivaid andmekaitsereegleid, võttes arvesse majanduse digitaliseerumist, uue tehnoloogiate kasutuselevõttu ning piiriüleste tehingute arvu kasvu.[68] Selleks võeti 27. aprillil 2016 vastu andmekaitse määrus.

Euroopa Komisjon defineeris andmekaitse määruse väljatöötamise käigus kolm peamist probleemide valdkonda, mida soovitakse lahendada: 1) liikmesriikide andmekaitse regulatsioonide killustatus, õiguslik ebaselgus ja ebaühtlane rakendamine põhjustavad takistusi ettevõtete tegutsemisele ja suurendavad avaliku sektori administratiivset koormust; 2) füüsilistel isikutel on keeruline oma isikuandmete töötlemist kontrollida; 3) puudused ja vastuolud isikuandmete kaitses seoses õiguskaitseasutuste koostöö käigus toimuva andmete töötlemisega.[69] Seega seati andmekaitse määruse üheks eesmärgiks andmekaitsealaste nõuete

[67] Andmekaitse direktiivi artikkel 14 punkt b teine lõik.
[68] Isikuandmete kaitse seaduse seletuskiri. 1026 SE. Justiitsministeerium, lk 3.
[69] *Ibid*.

ühtlustamine. Ühtlustamine omab olulist mõju isikuandmete töötlemise õiguslikele alustele, sealhulgas nõuetele, mis puudutavad ka kehtiva nõusoleku küsimist.

Andmekaitse määruse artikkel 6 lõige 1 sätestab, et isikuandmete töötlemine on seaduslik ainult juhul, kui on täidetud vähemalt 1 järgnevatest tingimustest:

1) andmesubjekt on andnud töötlemiseks oma nõusoleku;
2) töötlemine on vajalik lepingu täitmiseks või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele;
3) töötlemine on vajalik seadusjärgse kohustuste täitmiseks;
4) töötlemine on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks;
5) töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või avaliku võimu teostamiseks;
6) töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral.

Töötlemise alused pole seega direktiiviga võrreldes muutunud. Käesolev töö keskendub neist esimesele, isikuandmete töötlemisele nõusoleku alusel.

Kuna nõusoleku mõiste on aja jooksul edasi arenenud, täpsustab andmekaitse määrus kehtiva nõusoleku saamise aluseid, võttes aluseks andmekaitse direktiivi.[70] Määrusega artiklis 4 punktis 11 defineeritakse nõusolekut kui vabatahtlikku, konkreetset, teadlikku ja ühemõttelist tahteavaldust, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega. Nõusoleku mõiste sisuline võrdlus jääb käesoleva töö kolmandasse peatükki.

Andmekaitse määruse jõustumisega on lisaks vaja üle vaadata kehtiv IKS ning kõik siseriiklikud õigusaktid ja viia need määrusega vastavusse. Justiitsministeerium on ette valmistanud isikuandmete kaitse seaduse eelnõu, mis suuremas osas reguleerib õiguskaitseasutusi ning avaliku võimu kandjaid. Kehtiv IKS põhineb andmekaitse direktiivil, mis tunnistatakse andmekaitse määruse jõustumisega kehtetuks ning seda hakkab asendama otsekohalduv andmekaitse määrus. Siiski on liikmesriikidele andmekaitse määrusega jäetud võimalus reguleerida isikuandmete kaitset ulatuses, milles andmekaitse määrus on liikmesriikidele selle õiguse andnud. Selleks on välja töötamisel uus isikuandmete kaitse seadus ning isikuandmete kaitse rakendamise seadus. Seega ei saa 2018. a. IKS-i eelnõu käsitleda

[70] Ettepanek: Euroopa Parlamendi ja Nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaits eüldmäärus). Kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=COM:2012:0011:FIN.

määruses sätestatut, vaid üksnes täiendab ja täpsustab andmekaitse määruse sätteid määruses jäetud õiguse ulatuses. Kuna liikmesriikidele pole antud pädevus täpsustada nõusoleku formaalseid nõudeid, ei täpsusta 2018. a. IKS-i eelnõu selles osas küsimusi. Siiski on kehtestatud mõned erandid, millal töötlemine võib toimuda ilma nõusolekuta[71] ning muud erijuhud isikuandmete töötlemisel,[72] neid erandeid käsitleb töö autor peatükkides järgmises peatükis.

[71] Isikuandmete kaitse seadus. Eelnõu 21.03.2018, §-id 4-7.
[72] *Ibid*, §-id 8-10.

2. NÕUSOLEKU VAJADUS SÕLTUVALT TEISTEST ISIKUANDMETE TÖÖTLEMISE ALUSTEST ANDMEKAITSE MÄÄRUSES

2.1. Isikuandmete töötlemise üldised alused

Isikuandmete töötlemise läbiv põhimõte on olnud, et töötlemine võib toimuda üksnes õigusliku aluse olemasolul sõltumata sellest, kas töötlemine toimub Euroopa Liidu siseselt või väliselt.[73] Töötlemine võib toimuda nii vastutava kui volitatud töötleja poolt. Vastutav töötleja on see, kes määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid. Volitatud töötleja töötleb isikuandmeid vastutava töötleja nimel.[74]

Isikuandmetega toimingute tegemine on isikuandmete töötlemine. Andmekaitse määrus täpsustab artiklis 4 punktis 2, et isikuandmete töötlemine on isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine. IKS § 5 kohaselt on esitatud sarnane avatud loetelu töötlemise toimingutest.[75]Isikuandmete töötlemise mõistet isikuandmete kaitse seaduses ei ole võrreldes 2003. aastaga sisuliselt muudetud.[76]

Nii andmekaitse määruses kui ka IKS-i puhul on isikuandmete töötlemise mõiste puhul tegemist lahtise loeteluga, küll on aga andmekaitse määruses täpsustatud ulatuslikumalt, millised toiminguid töötlemiseks võib lugeda. Näiteks puudus isikuandmete kaitse seaduses sõnaselge viide sellele, et ka lugemine tähendab isikuandmete töötlemist. Viite puudumine ei välista siiski, et lugemine ei tähendaks isikuandmete töötlemist.

Isikuandmete töötlemisel peab järgima seaduslikkuse, eesmärgikohasuse, minimaalsuse, kasutuse piiramise, andmete kvaliteedi, turvalisus ja individuaalse osaluse põhimõtteid (IKS § 6).

---

[73] A. Bussche; P. Voigt. The EU General Data Protection Regulation, p 92.

[74] Euroopa Komisjon. Kes on vastutav töötleja või volitatud töötleja? Kättesaadav: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_et.

[75] IKS § 5 kohaselt on isikuandmete töötlemine iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest.

[76] E.Tikk ja A. Nõmper, lk 87.

Andmekaitse määruse kohaselt on isikuandmete töötlemiseks vaja andmete töötlejal alati õigusliku alust. Määrus näeb selleks ette 6 võimalust. Nimelt sätestab andmekaitse määruse artikkel 6 lõige 1, et isikuandmete töötlemine on seaduslik ainult juhul, kui on täidetud vähemalt 1 järgnevatest tingimustest:

1) andmesubjekt on andnud töötlemiseks oma nõusoleku;
2) töötlemine on vajalik lepingu täitmiseks või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele;
3) töötlemine on vajalik seadusjärgse kohustuste täitmiseks;
4) töötlemine on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks;
5) töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või avaliku võimu teostamiseks;
6) töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral.

Kehtiva IKS-i kohaselt on isikuandmete töötlemise õiguslikud alused § 12 lõike 1 ja § 14 lõike 1 alusel nõusolek, seadus, välisleping või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduv õigusakt, üksikisiku elu, tervise ja vabaduse kaitse ning leping. Eraldi alused kolmandale isikule andmete edastamiseks on sätestatud IKS § 14 lõikes 2, mille kohaselt edastamine on õigustatud, kui kolmas isik töötleb andmeid välislepingu või otsekohalduva õigusakti alusel, elu ja tervise kaitseks või teave on saadud avalike ülesandeid täites. Haldusorgani seaduslikud alused töötlemiseks on sätestatud muudest alusest eraldi (IKS § 10 lg 2).

Võrreldes kehtivat IKS-i andmekaitse määrusega sätestab viimane täiendavalt kaks uut õigusliku alust. Üheks selliseks õiguslikuks aluseks on andmesubjekti taotlus. Samuti on taas võimalik tugineda õigustatud huvile. Õigustatud huvi on küll IKS-i regulatsioonis varasemalt käsitletud, kuid võeti sealt 2004. aastal välja ning täna on sellele võimalik tugineda ainult väga piiratud juhtumil.

Andmesubjektil ei saa olla alati absoluutne õigus otsustada isikuandmete töötlemise üle nõusoleku andmise või selle tagasivõtmisega. Selleks ongi määrusega antud töötlejale võimalus kohaldada ka teisi sobivaid õiguslike aluseid, mis on konkreetse töötlemise puhul asjakohane. Töötlemisel võib esmapilgul tunduda, nagu kohalduma sobiks mitu õiguslikku alust, kuid

andmekaitse määruse alusel peab töötleja valima ühe kindla õigusliku aluse, millele tugineda.[77] Seega tuleb vaadata, millal on asjakohased muud õiguslikud alused peale nõusoleku.

2.2. Töötlemine lepingu alusel

Andmekaitse määruse artikkel 6 lõige 1 punkt b sätestab, et töötlemine on seaduslik juhul, kui see on vajalik andmesubjekti osalusel sõlmitud lepingu täitmiseks.

See säte hõlmab olukordi, kus isikuandmete töötlemine on vajalik, kuna andmesubjekti ja isikuandmete töötleja vahel on sõlmitud leping. Lepingu täitmiseks toimub töötlemine näiteks juhul, kui klient tellib e-poest kaupa ning soovib, et e-pood toimetaks talle kauba koju. Kliendil on vaja selleks e-poele esitada nimi ja kodune aadress ning paki kohale jõudmisest teada andmiseks ka kontakttelefon. Lepingu täitmise eesmärk andmete töötlemiseks väljendubki selles, et kliendile kaup koju tuua, vastasel juhul ei saa e-pood lepingut täita, kui ta neid andmeid töödelda ei saa.

Samas ei õigusta see alus lepingu alusel töötlemist siiski igas olukorras. Kui konkreetsel eesmärgil töötlemine pole lepingu jaoks vajalik, siis sellele alusele tugineda ei saa.[78] Näiteks pole leping sobiv õiguslik alus kasutaja profiili koostamiseks tema ostuklikkide põhjal veebileheküljel, kuna vastutav töötleja pole sõlminud lepingut profiilide koostamiseks, vaid kauba ja teenuse tarnimiseks. Seega profiili loomine pole kaupade ostmiseks ja kohale toimetamiseks sellise lepingu raames vajalik. Kui klient on kauba ära tellinud ja pole selle eest õigeaegselt tasunud, siis on lepingu täitmise eesmärgiga seotud näiteks kliendile meeldetuletuste saatmine arve tasumiseks.[79]

Ka seni kehtivas regulatsioonis on ühe töötlemise alusena ette nähtud leping (IKS § 14 lg 1 p 4). Kuna isikuandmete töötlemisel tuleb lähtuda eesmärgikohasuse põhimõttest (IKS § 6 p 2), on eelkirjeldatud eesmärke olnud vajalik eristada ka isikuandmete töötlemisel Eestis. Seega ei muutu põhimõte, mille kohaselt ettevõte võib kliendi isikuandmeid töödelda lepingu täitmiseks.

Lepingu täitmise eesmärgist tuleb eristada lepingu sõlmimisele eelnevate meetme võtmist. Andmekaitse määruse artikkel 6 lõige 1 punkt b sätestab selleks eraldi aluse, mille kohaselt isikuandmete töötlemine on seaduslik vastavalt andmesubjekti taotlusele lepingu sõlmimisele eelnevate meetmete võtmiseks.

[77] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 22.
[78] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 102.
[79] Article 29 Data protection Working Party, Opinion 06/2014, p 17-18.

Taotluse alusel töötlemisest saab rääkida näiteks siis, kui isik soovib saada pakkumist auto kindlustamiseks. Sellisel juhul on kindlustusandja õigustatud töötlema kliendi auto vanust ning muud vajalikku infot pakkumise tegemiseks.[80]

Arvestades näiteks finantsteenuse pakkuja tegevusega, on andmesubjektil teatud kohustus isikuandmete töötlemist taluda, kuid töötlemine peab seejuures vastama isikuandmete töötlemise põhimõtetele. Kui panga klient esitab laenu saamiseks panka taotluse on pangal vajalik taotluse läbivaatamiseks hinnata taotleja krediidivõimelisust vaadates üle kliendi varasemad tehingud. Seega on pakkumise tegemiseks vajalik paratamatult isikuandmeid töödelda. Sellise töötlemise õiguslikuks alus pole mitte aga taotlus andmekaitse määruse artikkel 6 lõike 1 punkti b alusel, vaid seadus või õigustatud huvi, kuna krediidivõimelisuse hindamine on oluline panga kohustuse täitmiseks, et kontrollida ametlike võlgnike nimekirju.[81] Eesti puhul siis näiteks maksuvõlgnike nimekirju.

Eesti seni kehtiv regulatsioon ei näe ette õigusliku alusena andmesubjekti taotlust. Seega pidi juhul, kui isik polnud veel lepingulisesse suhtesse astunud, küsima taotluses esitatud andmete töötlemiseks küsima nõusoleku. Leping kui töötlemise alus jääb alles, kuid ettevõtted saavad eraldi tugineda andmesubjekti taotlusele kui isikuandmete töötlemise õiguslikule alusele. Autori hinnangul saab lepingut kui töötlemise õigusliku alust sisustada sarnaselt praeguse regulatsiooniga, kuid ettevõtted peavad hakkama sisustama isikuandmete töötlemist andmesubjekti taotluse alusel.

2018. a. IKS-i eelnõu lepingu alusel töötlemist ei täienda. Seega jääb lepingu alusel töötlemise põhimõte sarnaseks kuni andmekaitse määruse jõustumiseni kehtiva isikuandmete regulatsiooniga. Seega ühe uue õigusliku alusena on ettevõtetel võimalik aga tugineda andmesubjekti taotlusele. Siiski võib eelnevate näidete puhul praktikas olla keeruline eristada, millal on õige tugineda andmesubjekti taotlusele või muule õiguslikule alusele, näiteks õigustatud huvile.

2.3. Töötlemine seaduse alusel

Andmekaitse määruse artikkel 6 lõike 1 punkist c tuleneb, et töötlemine on seaduslik, kui isikuandmete töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks. See tähendab, et seadusele saab õigusliku alusena tugineda töötleja siis, kui selline kohustus tuleb

[80] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. WP 217. Brussels: 2014. Available: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2, p 18.
[81] *Ibid*.

otsene viide seadusest. IKS-ist tuleneb seaduse alusel töötlemise lubatavus § 14 lõike 1 punktist 2.

Näiteks sätestab rahapesu ja terrorismi tõkestamise seadus[82] krediidiasutustele hulgaliselt kohustusi, mida krediidiasutused peavad järgima, et tõkestada Eesti Vabariigi rahandussüsteemi ning majandusruumi kasutamist rahapesuks ja terrorismi rahastamiseks. Rahapesu nõuete täitmiseks on krediidiasutustel lubatud seaduse rakendamisel kogutud isikuandmeid töödelda üksnes rahapesu ja terrorismi rahastamise tõkestamise eesmärgil (RahaPTS § 48 lg 2). See tähendab, et isikuandmete töötlemiseks eelnimetatud eesmärgil on õiguslikuks aluseks seadusjärgse kohustuse täitmine, mis tuleneb rahapesu ja terrorismi tõkestamise seadusest ning töötlemisel ei tohi selle eesmärgi piiridest väljuda.

Andmekaitse määrus ei sea ette piire siseriiklikule õigusele, selgitamaks, millal on õigustatud ja vajalik seaduse alusel isikuandmete töötlemine. Samas paljud alused, mil liikmesriik on teatavad kohustused ettevõtetele siiski kehtestanud, tulenevad kaudselt Euroopa Liidu õigusest. Näiteks eelmise näite puhul tuleneb rahapesu tõkestamise eesmärgil andmete töötlemise kohustus nn rahapesu tõkestamise direktiivist.[83]

Järelikult andmekaitse määruse kehtestamisega ei muutu nõuded, mis seonduvad isikuandmete töötlemisega seaduse alusel.

2.4. Töötlemine andmesubjekti eluliste huvide kaitseks

Andmekaitse määruse artikli 6 lõike 1 punktist d tuleneb, et isikuandmete töötlemine on lubatud juhul, kui see on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks. Sellel alusel on võimalik isikuandmeid edastada ka kolmandasse riiki.[84] Töötlemine, mis tugineb elulisele huvile, peaks aset leidma üksnes juhul, kui muule alusele tuginemine pole võimalik.[85] See tähendab, et elulisele huvile tuginemine on pigem teisejärguline, kuna enne elulise huvi erandi kohaldumist võib õigusliku aluse töötlemiseks kaasa tuua ka avalik huvi, kui töötlemine on vajalik humanitaareesmärkidel, sealhulgas

[82] Rahapesu ja terrorosmi tõkestamise seadus. Vastuvõetud 26.10.2017. RT I, 17.11.2017, 38.
[83] Euroopa Parlamendi ja Nõukogu direktiiv 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ. Kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32015L0849
[84] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 132.
[85] Andmekaitse määruse preambula punkt 46.

epideemia ja selle leviku jälgimiseks, või humanitaarolukordades, eriti loodusõnnetuste ja inimtegevusest tingitud õnnetuste korral.[86]

Isikuandmete töötlemine IKS § 14 lõike 1 punkti 3 alusel andmesubjekti elu või tervise kaitseks saab toimuda üksnes lisatingimusega, et andmesubjektilt ei ole mõistlikult võimalik nõusolekut saada (kui andmesubjekt pole kontaktivõimeline, teda pole võimalik mõistliku aja jooksul kätte saada või oleks andmesubjektilt nõusoleku küsimine ebamõistlikult raske). Andmekaitse määruses sellist eeldust pole eraldi sätestatud, küll aga võib mõistlikult eeldada, et eluliste huvide kaitsmine võib tulla ette olukorras, kus isikult pole nõusoleku küsimine mõistlikult eeldatav. Seega võib järeldada, et nõusoleku mitte-küsimine põhineb samadel eeldustel.

IKS-is sätestatud alusel võib andmesubjekti nõusolekuta olla erandjuhtudel lubatud tema isikuandmeid töödelda nii humanitaarabiga seonduvalt kui ka seoses arstiabi osutamisega (sh mitte ainult haige enda isikuandmeid, vaid ka teiste isikute andmeid – näiteks suguvõsas pärilike haiguste esinemisel võib andmesubjektile diagnoosi panemisel olla oluline teada, kas mõni tema lähedastest on vastavat haigust põdenud).[87] Seega sätestab andmekaitse määrus erinevuse humanitaarabi osas, milles määrus leiab, et töötlemise õiguslik alus on avalik huvi.

Siiski lubab andmekaitse määrus sarnaselt IKS-iga töödelda ka teise isikuandmeid, kui see on vajalik muu füüsilise isiku elulise huvi kaitseks. Seega kokkuvõtlikult saab järeldada, et andmekaitse määruse alusel isikuandmete töötlemise põhimõtted üldiselt ei erine IKS-is sätestatust, välja arvatud isikuandmete töötlemisel humanitaarolukordades.

2.5. Töötlemine avaliku huvi alusel

Andmekaitse määruse artikli 6 lõike 1 punkti e kohaselt on töötlemine lubatud juhul, kui see on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks. Seega katab andmekaitse määrus justkui kahte situatsiooni - avalik huvi ja avaliku võimu teostamine.

Avalikes huvides oleva ülesande täitmine on võimalik nii avalikes huvides loodud institutsiooni kui ka eraõigusliku juriidilise isiku poolt. Töötlemine peab olema avaliku huvi eesmärgil läbi viidava ülesande täitmiseks vajalik. Esiteks hõlmab see olukordi, kus vastutaval töötlejal endal on avalik võim või avalik huvi ning töötlemine on vajalik kõnealuse võimu teostamiseks või selle ülesande täitmiseks. Näiteks võib maksuhaldur koguda ja töödelda üksikisiku

[86] Andmekaitse määruse preambula punkt 46.
[87] Isikuandmete kaitse seaduse seletuskiri. 1026 SE. Justiitsministeerium, lk 15.

maksudeklaratsiooni, et kindlaks teha ja kontrollida makstava maksu suurust.[88] Samuti on avaliku ülesande täitmiseks isikuandmete töötlemisega tegemist siis, kui turvalisuse tagamiseks on vaja teostada video järelevalvet või jälgitakse kaameratega liikluses toimuvat.[89] Seega ei muuda avalik huvi teenuse olemasolu vastu seda veel iseenesest avalikuks ülesandeks.

Määrus ei selgita, millal on võimalik isikuandmete töötlemisel tugineda avaliku võimu teostamisele. Uue isikuandmete kaitse regulatsioonis on selgitatud, et avaliku võimu teostamisele on võimalik läheneda institutsionaalselt. Haldusmenetluse seadus sätestab §-s 8 haldusorgani mõiste, kes on seadusega, selle alusel antud määrusega või halduslepinguga avaliku halduse ülesandeid täitma volitatud asutus, kogu või isik. Lisaks haldusorganitele teostavad kõnesoleva seaduse mõttes avalikku võimu ka kohtud ja põhiseaduslikud institutsioonid. [90]

Eraõiguslikule juriidilisele isikule antakse avaliku võimu kandja volitused üle halduslepinguga. See, kuidas ja mil viisil halduslepinguga avaliku võimu üle saab anda, on samuti reguleeritud seadusega.

IKS § 10 lõike 2 alusel võib Eestis avaliku ülesande täitmise eesmärgil andmeid töödelda, kui see on ette nähtud kohustuse täitmiseks, mis tuleneb seadusest, välislepingust või otsekohalduvast õigustaktist. Eesti õiguses pole antud mõistetele avalikes huvides oleva ülesande täitmisele ja avaliku võimu teostamisele legaaldefinitsiooni. Kehtiv IKS-is tugineb üksnes isikuandmete töötlemise alusena avalikes huvides oleva ülesande täitmisele.

Andmekaitse määruses ei ole vahetegu ei ole isikuandmete töötlemisel avaliku huvi ja avaliku võimu teostamise alus päris selge. Vahetegu on keeruline, kuna kogu avaliku võimu tegevus tugineb seadustele ja määrustele. Kuna kehtivas IKS-is puudub viide töötlemisele avaliku võimu teostamiseks, tuleb artikli 6 lõike 1 punktile e tuginemiseks nende mõisted täpsemalt sisustada, mis ei ole käesoleva töö eesmärgiks.

2.6. Töötlemine õigustatud huvi alusel

Andmekaitse määruse artikkel 6 lõige 1 punkt f lubab isikuandmeid töödelda ka juhul, kui see on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud siis, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja –vabadused.

[88] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p 21.
[89] *Ibid*, p 22-23.
[90] Isikuandmete kaitse seaduse eelnõu seletuskiri. 06.11.2017. Justiitsministeerium, lk 8.

Õigustatud huvile saab ettevõte tugineda siis, kui õigustatud huvi on töötlemise õigustamise jaoks kõige sobilikum.[91] Õigustatud huvile tuginemiseks peab ettevõte võtma erilise vastutuse kindlustamaks, et andmesubjekti õigused ja huvid oleks siiski kaitstud. Huvi välja selgitamiseks peab ettevõte läbi tegema nö õigustatud huvi hindamise testi. Õigustatud huvi hindamise test koosneb kolmest alaosast. Esiteks, tuleb ettevõttel teha läbi eesmärgipärasuse test, et tuvastada ettevõtte õigustatud huvi (ing. k. *purpose test*). Teiseks tuleb viia läbi vajalikkuse test (ing. k. *necessity test*), et tuvastada, kas töötlemine on selle eesmärgi saavutamise jaoks vajalik. Kolmandaks, tuleb teha tasakaalustatuse test (ing. k. *balancing test*), et tuvastada ega üksikisiku huvid ei kaalu üle ettevõtte õigustatud huvi.[92]

Andmekaitse määrus ütleb, et õigustatud huvi alusel saab isikuandmeid töödelda pettuste vältimiseks ja otseturunduslikul eesmärgil.[93] Eelnev ei välista õigustatud huvile tuginemise muudel töötlemise eesmärkidel.

Andmekaitse töörühm on leidnud, et kolme testi tulemusena saab õigustatud huvile tugineda näiteks rikkumisest teavitamisel ehk vilepuhumisel ja IT turvalisuse tagamisel.[94] Õigustatud huvi alusel töötlemine on lubatud siiski senikaua, kuni töötlemise eesmärgid on seadusega kooskõlas.

Otseturunduse eesmärke pole aga andmekaitse määruses täpsustatud. Kuna otseturunduse mõiste on väga lai, siis tuleb selgitada, millist töötlemist saab läbi viia õigustatud huvi alusel. Ühe võimalusena on õigustatud huvi alusel töötlemine otseturunduse puhul lubatud juhul, kui heategevusorganisatsioon saadab posti teel olemasolevatele toetajatele infot organisatsiooni tegevuste kohta ning teateid tulevastest heategevusüritustest.[95] Samuti võib õigustatud huvile tugineda personaalsete turundusmaterjalide saatmisel e-kirja teel või veebilehel ja rakendustes kuvatavate reklaamide osas.[96] Seega on otseturunduse puhul õigustatud huvile tuginemine lubatud siis, kui edastav info on seotud ettevõte ja kliendi varasema suhtega ning andmesubjekt võiks seda mõistlikult oodata.

Selleks, et kindlaks teha, millistel juhtudel võib otseturunduse puhul tugineda õigustatud huvile ning kas on töötlemiseks vaja ehk mõnda muud alust, tuleb vaadata ka Euroopa Parlamendi ja

[91] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p 48.
[92] Data Protection Network. Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation .2017, p 14.
[93] Andmekaitse määruse preambula punkt 47.
[94] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p 25.
[95] Data Protection Network. Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation. 2017. p12.
[96] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p. 103-104.

Nõukogu määruse ettepanekut, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (edaspidi e-privaatsuse määrus). Nimelt on andmekaitse määruse kõrval oluline ka uus e-privaatsus määrus, mille vastu võtmine lükkub 2019. aastasse.[97]

E-privaatsuse määruse artikkel 16 lõige 1 sätestab, et füüsilised või juriidilised isikud võivad kasutada elektroonilise side teenuseid, et saata otseturundusteadaandeid füüsilisest isikust lõppkasutajatele, kes on andnud selleks oma nõusoleku. See tähendab, et e-privaatsuse määrusega ei muutu juba varem kehtinud põhimõte, et otseturundusteadete edastamiseks elektroonilise side teenuste kaudu on vaja nõusolekut. Nõusoleku vajadusest otseturunduse eesmärgiks käsitletakse peatükis 2.9.4.

Tänases IKS-is õigustatud huvi õigusliku alusena on ette nähtud üksnes isikute krediidivõimelisuse hindamiseks või muul samasugusel eesmärgil kolmandatele isikutele edastamiseks (IKS § 11 lg 6). Kuna täna IKS-is on õigustatud huvi ette nähtud üksnes krediidivõimelisuse hindamisega seonduvalt, saab väita, et tegemist on justkui üle 14 aasta uue õigusliku alusega isikuandmete töötlemiseks. Samas oli turuosalistel ka kehtiva regulatsiooni valguses võimalik asuda seisukohale, et õigustatud huvi alusel töötlemine on võimalik otse andmekaitse direktiivile tuginedes, juhul kui liikmesriigil oli kohustus see alus siseriikliku õigusesse üle võtta, kuid Eesti riik seda ei teinud. Kuna nõusoleku saamine võib olla keeruline, võib ettevõtete jaoks olla lihtsam tugineda õigustatud huvile, kui on läbitud õigustatud huvi hindamise test.

2.7. Töötlemine nõusoleku alusel

2.7.1. Nõusoleku alusel töötlemise üldised alused

Nõusolek isikuandmete töötlemiseks on vajalik juhtudel, mil ükski teine artikli 6 lõikes 1 toodud alus ei sobi isikuandmete töötlemise õiguslikuks aluseks.[98] Seega enne nõusolekule tuginemist tuleb kontrollida, kas töötlemist võib õigustada mõne muu õigusliku alusega.

Üldise põhimõtte kohaselt on ettevõttel nõusolekut vaja siis, kui kasutamine väljub esialgsest eesmärgist.[99] Seda kinnitab andmekaitse määruse artikli 6 lõike 1 punkt a, mille kohaselt

[97] E-Privacy Regulation will not come into force until 2019. Press relase, 24.11.2017. Available: https://www.eprivacy.eu/en/about-us/news-press/news-detail/article/eprivacy-regulation-will-not-come-into-force-until-2019/.
[98] Information Commissioner's office. Consultation: GDPR consent guidance, p 12.
[99] *Ibid*.

andmesubjekti nõusolek tuleb anda ühel või mitmel konkreetsel eesmärgil, mis tähendab, et andmesubjektil on võimalus iga eesmärgi puhul kaaluda nõusoleku andmist.

Näiteks tuleb nõusolek küsida, kui soov saata andmesubjektile reklaami, turu-uuringute küsitlusi[100] ja kasutada isikust pilti ajakirja kaanel.[101]

Kuna põhimõte, et isikuandmete töötlemine on lubatud muuhulgas nõusoleku alusel, ei ole muutunud, siis saab nõusoleku vajadust selgitada ka andmekaitse direktiivi tõlgenduste abil.

Andmekaitse direktiivi artikli 6 lõike 1 punkti b kohaselt tuleb isikuandmeid koguda täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid tohi hiljem töödelda viisil, mis on nende eesmärkidega vastuolus. Kui töötleja kavatseb töödelda andmeid eri otstarvetel, on nõusolekut vaja siiski igaks otstarbeks. Näiteks võib nõusoleku küsida viisil, mis kataks ära nii uutest toodetest teavitamise kui ka konkreetsed müügiedendusmeetmed, kuna seda võiks pidada andmesubjekti põhjendatud ootustele vastavaks. Kuid selleks, et võimaldada üksikisiku andmete saatmist kolmandatele isikutele, tuleks nõuda eraldi ja täiendavat nõusolekut.[102] Seega tuleb igal üksikjuhtumil eraldi hinnata töötlemise eesmärki, mille kohta on konkreetselt nõusolekut vaja ning mille tulemusel saab järeldada, kas vajalik on üks või mitu nõusolekut.

Ka Eesti õiguses on selgitatud, et isikuandmete töötlemisel üheks eesmärgiks kogutud andmed ei sobi ilma andmesubjekti täiendava nõusolekuta üldjuhul muude eesmärkide saavutamiseks. See tuleneb minimaalsuse, kasutuse piiratuse ning eesmärgipärasuse põhimõtetest.[103]

Lisaks sellele, et nõusoleku vajadust ja eesmärke tuleb hinnata ja eristada kliendisuhte alguses, tuleb töötlemise eesmärke üle hinnata ka jooksvalt. Kui töötlemise eesmärgid on ajas muutunud, tuleb kasutajaid uuesti eesmärkidest teavitada ning anda neile võimalus nõustuda uue andmete töötlemise eesmärgiga.[104]

Kui ettevõte soovib kliendiandmeid kasutada hiljem statistilise analüüsi tegemiseks klientide ostuharjumuste kohta, pole selle jaoks uut nõusolekut vaja, kui statistika analüüsi tulemust või

[100] Õiguskantsleri märgukiri KindlTS § 14^2 lg 2 ja KAS § 89 lg 2^2 ja 2^3 põhiseaduspärasus. 26.02.2014, lk 7. Kättesaadav: http://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_oigus_votta_nousolek_isikuandmete_tootlemiseks_tuuptingimustes.pdf.
[101] EIKo, 20.06.2017, 13812/09, *Bogomolova* vs. *Russia*.
[102] Fundamental Rights Agency, p 67.
[103] A. Henberg, Isikuandmete töötlemine töösuhtes. Juridica 2005, nr 8, lk 563.
[104] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679. WP 259. Brussels: 2017, p. 12. Available: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239.

isikuandmeid ei kasutata ühtegi konkreetset füüsilist isikut puudutavate meetmete või otsuste toetamiseks.[105]

Isikuandmete kaitse seaduse § 10 lõikes 1 on sätestatud, et isikuandmete töötlemine on lubatud üksnes andmesubjekti nõusolekul, kui seadusest ei tulene teisiti. Seega Eesti õiguses täna IKS justkui prioritiseerib nõusolekut, mis tähendab, et isikuandmete töötlemiseks on õiguslikest alustest eelkõige vajalik andmesubjekti nõusolek. On kaheldav, kas direktiiv on kohustanud sellist prioriteetsust seadma.[106] Seega on sellise prioriteetsuse seadnud Eesti ise.

Eesti kohtupraktikas on leitud, et ka siis, kui isik on ise enda kohta käivaid isikuandmeid avalikustanud, ei saa nende korduval avalikustamisel või töötlemisel siiski IKS § 11 lõikele 1 tugineda, mistõttu ka avalikustatud andmete kasutamiseks on vajalik seaduslikku alust, milleks võib olla andmesubjekti nõusolek.[107] Teisalt on kohtupraktikas leitud, et IKS-i kohane nõusolek pole nõusolek VÕS § 1045 lg 2 p 2 mõttes. [108]

2.7.2. Nõusoleku alusel töötlemise erijuhud

Andmekaitse määrus näeb konkreetselt ette mõned juhud, millal võib isikuandmete töötlemine toimuda üksnes nõusoleku alusel:

1) infoühiskonnateenuse pakkumisel lapsele (artikkel 8 lõige 1);
2) eriliigiliste isikuandmete töötlemisel (artikkel 9 lõige 2 punkt a);
3) isikuandmete edastamisel kolmandale riigile või rahvusvahelisele organisatsioonile, kui sellega pole tagatud piisav kaitse (artikkel 49 lõige 1 punkt a).
4) automatiseeritud otsuste puhul ehk kui andmeid töödeldakse automaatselt ning see toob endaga kaasa andmesubjekti puudutavaid õiguslikke tagajärgi või avaldab talle märkimisväärset mõju (artikkel 22 lõige 2 punkt c);

Lisaks peatükis 2.6. käsitletule, tuleb käsitleda ka nõusoleku vajadust otseturunduse puhul. Neid konkreetseid erijuhtumeid käsitletakse järgmises alapeatükis.

2.7.2.1. Infoühiskonna teenuse pakkumine lapsele

Andmekaitse määrus näeb vajalikuks laste isikuandmeid eriliselt kaitsta, kuna lapsed ei pruugi olla piisavalt teadlikud asjaomastest ohtudest, tagajärgedest ja kaitsemeetmetest ning oma õigustest seoses isikuandmete töötlemisega. Selline kaitse on eelkõige vajalik laste

[105] Fundamental Rights Agency, lk 68.
[106] Lee A. Bygrace. Data Privacy Law. An International Perspctive, p 161.
[107] RKTKo 3-2-1-159-14 p 14.
[108] RKTKo. 3-2-1-153-16.

isikuandmete kasutamisel turunduse eesmärgil või isiku kasutajaprofiili loomiseks ja otse lastele pakutavate teenuste kasutamise puhul.[109] Otse lastele pakutavate teenuste all ei mõelda selliseid teenuseid, mida saavad küll muuhulgas lapsed kasutada, kuid pole eelkõige neile suunatud - näiteks riideid müüv e-pood. Selle mõiste alla võib aga kuuluda koolidele suunatud veebipõhine entsüklopeedia.[110]

Kaitse tagamiseks näeb andmekaitse määruse artikkel 8 lõike 1 esimene lause ette, et pakkudes otse lapsele infoühiskonna teenust, on lapse isikuandmete töötlemine seaduslik ainult juhul, kui laps on vähemalt 16-aastane. Artikli 8 lõike 1 teises lauses on lisatud, et alla 16-aastase lapse isikuandmete töötlemine on seaduslik siis, kui nõusoleku või loa andnud isik, kellel on lapse suhtes vanemlik vastutus. Lisaks näeb andmekaitse määrus veel samas sättes ette liikmesriikidele võimaluse langetada seadusega vanusepiir kuni 13-aasta vanuseni.

Infoühiskonna teenus on kõik vahemaa tagant elektroonilisel teel ja teenusesaaja isikliku taotluse alusel ning tavaliselt tasu eest osutatavad teenused.[111] Mõiste kattub üldjoontes infoühiskonna teenuse seaduses sätestatud infoühiskonna teenuse mõistega, kuigi infoühiskonna teenuse seaduses tasu ei eeldata.[112] Vahemaa tagant tähendab seda, et teenust osutatakse ilma poolte üheaegse kohalolekuta. Elektroonilisel teel tähendab, et teenus saadetakse lähtepunktist ja võetakse sihtkohas vastu elektrooniliste andmetöötlus- ja säilitusseadmete abil ning see saadetakse, edastatakse ja võetakse vastu täielikult juhtmete või raadio kaudu, optiliselt või muude elektromagnetiliste vahendite abil. Lühidalt öeldes hõlmavad infoühiskonna teenused lepinguid ja muid teenuseid, mis on sõlmitud või edastatud internetivõrgus.[113] Vanema nõusolekut ei ole vaja juhul, kui lapsele pakutakse otse ennetavaid või nõustamisteenuseid.[114]

Lapse isikuandmete töötlemisel võib ettevõtetel, kes osutavad teenust läbi interneti, problemaatiliseks osutuda lapse vanuse tõendamine, kuna internetis uue kasutajalehega liitumisel võib olla keeruline tuvastada, kes on nö teisel pool ekraani. See tähendab, et ka sotsiaalmeedia kasutamiseks peab olema vanema nõusolek. Esiteks peab ettevõte tuvastama,

[109] Andmekaitse määruse preambula punkt 38.
[110] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 99.
[111] Andmekaitse määruse artikkel 4 punkt 25 viitab infoühiskonna teenuse mõiste sisustamisel Euroopa Parlamendi ja nõukogudirektiivi (EL) 2015/1535 (1) artikli 1 lõike 1 punktile b.
[112] Infoühiskonna teenuse seaduse § 2 p 1 kohaselt on Infoühiskonna teenuse puhul tegemist teenusega, mida osutatakse majandus- või kutsetegevuse raames teenuse kasutaja otsesel taotlusel ja mille puhul andmeid töödeldakse, säilitatakse ja edastatakse digitaalkujul andmete töötlemiseks ja säilitamiseks mõeldud elektrooniliste vahendite abil, kusjuures osapooled ei viibi üheaegselt samas kohas. Infoühiskonna teenus peab olema täielikult üle kantud, edastatud ja vastu võetud elektrooniliste sidevahendite abil.
[113] EKo 02.12.2010, C-108/09, *Ker-Optika* § 22 ja 28.
[114] Andmekaitse määruse preambula punkt 38.

kui vana on ankeedi täitja. Selleks peab ettevõte enne veebilehega liitumist küsima, kui vana isik on. Üle Euroopa tegutseva ettevõtte jaoks on see eriti problemaatiline juhul, kui ettevõte peab järgima kõikide tarbijate asukohariikide õigust, kuna lapse nõusolekule saavad liikmesriigid sätestada erinevad vanuseastmed, mis hetkeni on vanema nõusolekut vaja. Ühe võimalusena saab ettevõtevastava vanuse nõuded ära kaardistada sõltuvalt sellele, mis riigis ta teenust pakub ning teenusega liitudes paluda kliendil ära märkida oma elukohajärgne riik. Kuna andmekaitse määruse artikkel 8 lõige 3 märgib aga, et lõikest 1 tulenevad nõuded ei mõjuta liikmesriikide üldist lepinguõigust, siis võib ettevõte rakendada kõigile ühesuguseid nõudeid ning nõuda kõigilt alla 16-aastastelt isikutelt vanema nõusolekut.

Teiseks probleemkohaks on see, et ettevõte peab olema kindel, et vanem on lapse isikuandmete töötlemisega nõustunud. Seega peab ettevõttel olema vanema nõusolek. Andmekaitse määruse artikkel 8 lõige 2 näeb ette, et ettevõte peab tehnoloogiat arvesse võttes tegema mõistlikud jõupingutused tuvastamaks, et nõusoleku on andnud vanem. Andmekaitse töörühm on leidnud, et töötleja peaks koguma vähemalt vanema kontaktandmed.[115] Järelikult pole alaealise puhul piisavaks meetmeks see, kui veebilehekülgega liitumise all on kast, kuhu tuleb vajaduse korral lisada linnuke, mille kohaselt kinnitatakse vanema nõusolekut.

Samas tuleb arvesse võtta konkreetse töötlemise laadi, ulatust, konteksti ja eesmärki tuvastamaks, kui suurt riski endas antud töötlemine kannab (andmekaitse määruse art 35 lg 1). Selleks, et tuvastada nii isiku vanus kui saada vanema nõusolek, võib madala riskiga juhtudel olla piisav vanema kinnitus e-kirja teel. Kõrgema riskiga juhtudel tuleb kasutusele võtta täiendavaid meetmeid. Näiteks, kui isik soovib liituda veebipõhise kihlveoportaaliga, peab portaal küsima, kas isik on vähemalt 16. aasta vanune. Kui ta ütleb, et ei ole 16. aasta vanune, siis portaal teavitab, et teenuse kasutamiseks on vaja vanema nõusolekut ning palub selleks edastada vanema e-posti aadress. Portaal võtab seejärel vanemaga ühendust ning küsib nõusolekut.[116] Siiski jääb kohtupraktika kujundada, mida loetakse mõistlikeks pingutusteks, kuna määruse alusel on see veel ebaselge. Kõnealuse näite puhul tuleb muidugi arvesse võtta ka siseriiklike nõudeid, mis võivad ette näha piiranguid kihlveo pakkumistel osalemisteks.

Eestis kehtiva õiguse kohaselt ei sätesta IKS alaealise puhul ise vanema nõusoleku vajaduse juhtumeid, vaid viitab tsiviilseadustiku üldosa seadusele. Tsiviilseadustiku üldosa seadus sätestab tehingule täiendavad nõuded isiku puhul, kes on alla 18-aasta vanune ning seega piiratud teovõimega (TsÜS § 8 lg 2). Järelikult tuleb teha kindlaks, kas nõusolek on tehing.

[115] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 25.
[116] *Ibid*, p 26.

Nõusoleku andmine toob endaga kaasa isikuandmete töötlemise, mis tähendab, et andmesubjekti nõusolek on selge ja teadlik andmesubjekti tahteavaldus, millega ta lubab oma isikuandmeid töödelda.[117] Seega vastab nõusolek tehingu mõistele.[118] Sellist tahteavaldust saab väljendada üksnes täielikult teovõimeline isik. Piiratud teovõimega isiku puhul on vajalik seega seadusliku esindaja nõusolek, kelleks alaealise puhul võib olla vanem või eestkostja või peab seaduslik esindaja andma nõusoleku andmiseks oma nõusoleku või selle hiljem heaks kiitma.

Seega ei muutu Eesti õigusest üldiselt tulenev põhimõte, et lapse isikuandmete töötlemiseks on vajalik esindaja nõusolekut. Need piirid määrab endiselt tsiviilseadustik. Samas polnud seni sätestanud IKS-is eraldi nõusoleku nõuet lapsele infoühiskonnateenuste pakkumisel. Kuna sotsiaalmeedias toimub isikuandmete töötlemine, siis see ei tähenda, et nõusolekut poleks seni vaja olnud. Kui ettevõtted pole varasemalt lapse poolt sotsiaalmeedia kasutamiseks vanema nõusolekut võtnud, siis andmekaitse määruse järgi tuleb seda kindlasti teha.

IKS-i kohaselt on seega seadusliku esindaja nõusolek vajalik igal juhul, kui toimus lapse isikuandmete töötlemine. See põhimõte jääb ka andmekaitse määrusega kehtima, kuna määrusest tulenevad üldised nõuded kehtivad ka laste isikuandmete töötlemisele. Kuigi määrus ei reguleeri esindusõigust, siis esindaja nõusoleku vajadus tuleneb endiselt tsiviilseadustiku üldosa seadusest.

2018. a. IKS-i eelnõus on kehtestatud töötlemise lubatavuse piiriks, kui isik on vähemalt 13-aastane (2018. a. IKS-i eelnõu § 8 lg 1). Madalama vanusepiiri kehtestamisega uues isikuandmete kaitse seaduses oleks tegemist erisätteks TsÜS § 8 lõikele 2, kuid seda üksnes juhtudel, mis seotud infoühiskonna teenuse pakkumisega.

Andmekaitse määrusest tõusetub lapsele infoühiskonna teenuse pakkumisel seega 3 probleemkohta. Esiteks peavad ettevõtted selgitama andmekaitse määruse mõjualas olevates riikides sätestatud erinevad vanusepiirid. Teiseks, jääb ebaselgeks, palju ettevõtted peavad vaeva nägema, et vanemaga ühendust saada. Kolmandaks, peab välja selgitama, milline on mõistlik pingutud, mida ettevõtted peavad tegema, et teada saada, kui vana on teisel pool ekraani olev isik.

[117] Isikuandmete kaitse seaduse seletuskiri. 1026 SE, lk 13.
[118] TsÜS 67 lõike 1 kohaselt on tehing toiming või omavahel seotud toimingute kogum, milles sisaldub kindla õigusliku tagajärje kaasatoomisele suunatud tahteavaldus.

2.7.2.2. Eriliigiliste isikuandmete töötlemine

Andmekaitse määrus eristab tavalisi isikuandmeid ja isikuandmete eriliikide ehk senise definitsiooni järgi IKS-is delikaatseid isikuandmeid.

Isikuandmete eriliigid on teatavat liiki isikuandmed, mille laadist tulenevalt võidakse nende töötlemise korral andmesubjekt ohtu seada ning mis seetõttu vajavad tugevdatud kaitset.[119] Eriliigilised isikuandmed on andmekaitse määruse mõistes isikuandmeid, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, terviseandmeid või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta (andmekaitse määruse art 9 lg 1).

Andmekaitse määruse artikkel 9 lõike 2 punkti 2 kohaselt on ette nähtud, et eriliigiliste isikuandmete töötlemine on lubatud ühe võimalusena andmesubjekti selgesõnalisel nõusolekul. Samas võib tundlike isikuandmete töötlemine olla lubatud ka eluliste huvide, õigustatud huvi ja avaliku huvi raames.[120]

Kehtiv IKS jagab sarnaselt andmekaitse määrusega isikuandmed kahte gruppi ehk tavalisteks isikuandmeteks ja delikaatseteks isikuandmeteks. Eristuse aluseks on andmete sisu ning sisust tuleneva riive intensiivsus. [121] Delikaatsete isikuandmete sisu IKS § 4 lõike 2 mõistes üldjoontes kattub andmekaitse määrusega. Seega saab järeldada, et delikaatsete isikuandmete ja isikuandmete eriliikide all mõeldakse sisuliselt sama asja.

Üldiselt on tegemist IKS-is kinnise loeteluga, v.a. biomeetriliste andmete osas, mille suhtes on tegemist avatud loeteluga (IKS § 4 lg 2 p 5). Erinevusena puudub andmekaitse määruse loetelust ühe liigina süüteo toimepanemine või selle ohvriks langemine enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist. See alus on jäetud välja ka 2018. a. IKS-i eelnõust. Seletuskirjas pole küll välja jätmist põhjendatud aga selle andmete liigi puhul võib problemaatiline olla asjaolu, et kui kohtuistung on avalik, siis ei saa neid andmeid enam delikaatseteks lugeda.[122]

Isikuandmete eriliikide töötlemine toimub näiteks elukindlustusjuhtumi raames. Seega peab isik enne elukindlustuse sõlmimist andma kindlustusandjale selgesõnalise nõusoleku tema terviseandmeid puudutavate isikuandmete töötlemiseks. Kui kindlustusjuhtum on saabunud

[119] Fundamental Rights Agency, p 41.
[120] *Ibid*, p 86-87.
[121] M. Männiko, lk 42.
[122] RKo 3-3-1-3-12, p 19.

ning andmesubjekt soovib, et kindlustusandja hüvitaks talle tekkinud kulud, siis saab kindlustusandja tugineda tema varasemale nõusolekule. See tähendab ühtlasi, et kui isik võtab nõusoleku tagasi, siis pole tal ka õigust elukindlustusjuhtumi tõttu tekkinud kahju hüvitamisele.

Kui andmesubjekt on ise need andmed avalikustanud, pole selgesõnalist nõusolekut töötlemiseks vaja, kuna avalikustamine vihjab sellele, et andmesubjekt on nõus andmete kasutamisega.[123]

Biomeetriliste andmete hulgas on küsitav, kas ka fotot võib biomeetrilisteks andmeteks lugeda. Biomeetriliste andmete mõistest tuleneb, et sellisteks andmeteks on muuhulgas näokujutis, mis saadud tehnilise töötlemise abil. See tekitab küsimuse, kas tavaline foto langeb kõnealuse mõiste alla, kuna sellisel juhul võib ka üliõpilaspileti tegemiseks olla vaja isiku selgesõnalist nõusolekut. Andmekaitse määruses on siiski selgitanud, et fotode töötlemist ei peaks süstemaatiliselt käsitlema isikuandmete eriliikide töötlemisena, kuna need on hõlmatud biomeetriliste andmete määratlusega üksnes siis kui neid töödeldakse konkreetsete tehniliste vahenditega, mis võimaldavad füüsilist isikut kordumatult tuvastada või autentida.[124] See tähendab, et fotot saab lugeda biomeetriliseks andmeteks näiteks passipildi puhul, kuna tänane tehniline lahendus suudab passipildi pealt tuvastada passikontrollis isiku näokujutise. Avaliku võimu raames teostatav isikuandmete töötlemine ei kuulu käesoleva töö eesmärgi alla, mistõttu ei lasku töö autor siin detaili selgitamaks, kas sellise töötlemise jaoks on vaja nõusolekut või saab isikuandmete töötlemisel tugineda avalikule huvile.

Ühe erandina on võimalik eriliigilisi isikuandmeid töödelda siiski juhul kui see on vajalik õigusnõuete koostamiseks, esitamiseks või kaitsmiseks sõltumata sellest, kas see toimub kohtumenetluse, haldusmenetluse või kohtuvälise menetluse raames.[125] Täna on selline õigus sätestatud advokatuuriseaduse § 42 lõikes 4^1 mille kohaselt advokaat võib töödelda ilma andmesubjekti nõusolekuta eriliigilisi isikuandmeid.

Põhjusel, et ka IKS eristab delikaatseid isikuandmeid tavalistest, siis on ka eraldi sätestatud töötlemise alus, mille kohaselt ettevõte peab kõigepealt isikule selgitama, et tegemist on delikaatsete isikuandmetega ning nende töötlemiseks peab võtma andmesubjekti kirjaliku taasesitamist võimaldava nõusoleku (IKS § 12 lg 4). Seda, kas selgesõnalisuse nõue toob kaasa muutuse seni delikaatsete isikuandmete töötlemisel analüüsib töö autor lähemalt 3.5. peatükis.

[123] Fundamental Rights Agency, p 86.
[124] Andmekaitse määruse preambula punkt 58.
[125] Andmekaitse määruse preambula punkt 52.

2018. a. IKS-i eelnõu aga sätestab eriliigilistele isikuandmetele teise lähenemise. Nimelt on eriliiki isikuandmete töötlemine on lubatud ainult juhul, kui töötlemise alus tuleb seadusest, vajalik andmesubjekti või teise füüsilise isiku eluliste huvide kaitseks või andmesubjekt on need avalikustanud. Selline lähenemine võimaldab eriliigilisi isikuandmeid töödelda näiteks õiguskaitseasutustel.[126]

Kuna andmekaitse määruse loetelusse pole lisatud uusi mõisteid, millest tulenevalt võiks eriliigiliste andmete käsitlus muutuda, saab järeldada, et selles osas jääb regulatsioon varasemaga võrreldes samasuguseks.

2.7.2.3. Isikuandmete edastamine kolmandale riigile või rahvusvahelisele organisatsioonile, kui sellega pole tagatud piisav kaitse

Andmekaitse määruse artikli 49 lõike 1 punkti a kohaselt on vaja andmesubjekti selgesõnalist nõusolekut juhul, kui tema isikuandmeid edastatakse kolmandatesse riikidesse või rahvusvahelisele organisatsioonile ning sellega võivad kaasneda ohud, mis tulenevad kaitse piisavuse otsuse ja asjaomaste kaitsemeetmete puudumisest. Näiteks kui puuduvad siduvad kontsernisisesed eeskirjad. Kõnealune säte lubab andmesubjekti nõusolekul andmeid kolmandale riigile või rahvusvahelisele organisatsioonile edastada ühe- kui mitmekordselt.[127]

Kolmandad riigid on riigid, mis jäävad väljapoole Euroopa Liitu. Siiski on osad riigid väljaspool Euroopa Liitu tuvastatud turvaliseks. Selline volitus on antud Euroopa Komisjonile.[128] Näiteks on turvalised riigid Andorra, Argentiina, Kanada. Samuti loetakse turvalisteks kolmandateks riikides riigid, mis on Euroopa Majanduspiirkonnas (Island, Lichtenstein, Norra).[129]

Isegi, kui ettevõttel on juba isikuandmete töötlemiseks määruse artiklile 7 vastav nõusolek olemas, siis ei saa ta andmete kolmandasse riiki edastamiseks piisavate turvameetmete puudumisel kasutada varem küsitud nõusolekut, vaid edastamiseks peab olema eraldi nõusolek. Kui andmete töötlejal on kohe teada, et andmeid edastatakse ka kolmandale riigile, siis võib tulla kõne alla nõusoleku eesmärkide ühendamine. Kui aga kogumise hetkel seda teada polnud, on vaja eraldi nõusolekut. [130]

[126] Isikuandmete kaitse seaduse eelnõu seletuskiri. 06.11.2017, lk 26.
[127] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 118-119.
[128] Andmekaitse määruse preambula punkt 103.
[129] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 116-118.
[130] Guidelines on Article 49 of Regulation 2016/679, WP 261. 6 February 2018, p 7.

Kehtivas isikuandmete kaitse regulatsioonis on käsitletud sarnaselt isikuandmete edastamist välisriiki. IKS näeb ette, et seal, kus pole piisav andmekaitse tase tagatud, peab ettevõte sellisesse riiki edastamisel küsima andmesubjekti käest nõusoleku (IKS § 18 lg 5 p 1). Seega ei muutu nõusoleku vajadus andmete saatmisel ebapiisavate kaitse meetmetega riiki.

2.7.2.4. Automatiseeritud otsused

Andmekaitse määruse artikkel 22 lõige 1 sätestab, et andmesubjektil on õigus, et tema kohta ei võetaks otsust, mis põhineb üksnes automatiseeritud töötlusel, sealhulgas profiilianalüüsil, mis toob kaasa teda puudutavaid õiguslikke tagajärgi või avaldab talle märkimisväärselt mõju. See tähendab, et automatiseeritud töötlusel põhinev otsus, mis toob andmesubjektile kaasa õiguslikke tagajärgi või avaldab talle märkimisväärset mõju, on andmekaitse määruse kohaselt keelatud.[131] Artikkel 22 lõige 2 täpsustab, et automaatsel töötlusel põhinev otsus on lubatud juhul, kui see on vajalik andmesubjekti ja vastutava töötleja vahelise lepingu sõlmimiseks või täitmiseks või kui see on lubatud liikmesriigi õigusega või põhineb andmesubjekti selgesõnalisel nõusolekul.

Selleks, et saada teada, millal on tegemist automaatse otsusega, mille puhul on vaja nõusolekut, peab esmalt avama automatiseeritud töötlemise ja profiilianalüüsi sisu.

Profiilianalüüs on andmekaitse üldmääruse artikli 4 punkti 4 mõistes igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud asjaomase füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega. Automatiseeritud töötlemine on töötlemise vorm, mis hõlmab mingit automatiseeritud töötlemist näiteks arvuti poolt, kuigi inimsekkumine ei välista, et tegemist oleks automatiseeritud töötlemisega.[132]

Enamikel juhtudel ei oma sihtgrupi järgi tehtud pakkumised üksikisikutele olulist mõju. Samas on vastupidine võimalik sõltuvalt profiilianalüüsi protsessi sekkumise ulatusest, üksikisiku soovidest ja huvidest, reklaami edastamise viisist ning andmesubjekti haavatavusest.[133]

---

[131] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 180.
[132] Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. WP 251. Brussels: 2017, p 6. Available: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
[133] *Ibid*, p 11.

Automatiseeritud töötlusel põhinevast otsusest saab rääkida siis, kui otsuse tegemise protsessis puudub inimsekkumine.[134] Nagu eelnevalt öeldud, võib üldiselt automatiseeritud töötlus sisaldada mingil määral inimsekkumist, kuid kõnealuse sätte puhul on rõhutatud, et otsus peab põhinema üksnes automatiseeritud töötlemisel. Sellest saab järeldada, et kui isikuandmete töötlemisel annab oma panuse ka inimene, siis artikkel 22 ei kohaldu.

Praktikas võivad automatiseeritud otsusteks olla otseturunduspakkumised, mis viivad lepingu sõlmimiseni. Näiteks kui panga kliendile kuvatakse eelarvutatud limiidiga pakkumisi, mis tehtud konkreetse kliendi varasid ja kohustusi arvesse võttes. Eelarvutatud limiidiga pakkumise puhul tuleb esmalt hinnata, kas eelarvutatud limiidiga pakkumised on automatiseeritud töötlemisel põhinevad otsused.

Kui klient näeb panga kodulehel eelarvutatud limiidiga pakkumist, siis sellisel juhul õiguslik tagajärg, mis võib kaasneda, on leping. Samas ei too autori hinnangul ainuüksi pakkumise kuvamine kliendile õigusliku tagajärge kaasa, kui klient lepingut ei sõlmi. Seega pole pakkumine üksi automatiseeritud töötlusel põhinev otsus ning sellele ei pea kohaldama artikli 22 nõudeid.[135] Automatiseeritud töötlusel põhineva otsusega on tegemist siis, kui klient soovib pakkumisest otse lepingulisesse suhtesse astuda. Seega peab nende kahe etapi vahel olema kliendil võimalik valida, kas nõustub automatiseeritud töötlusel põhineva otsusega või nõuab inimsekkumist.

Samas kui automatiseeritud töötluse puhul on tehtud otsus klientide osas, kellele eelarvutatud limiidiga pakkumist mitte kuvada, tekib küsimus, kas kaasnenud on samuti õiguslik tagajärg ehk panga otsus kliendile mitte laenu anda. Selleks tuleb selgitada, mida tähendab määruses, et automatiseeritud töötlus avaldab andmesubjektile märkimisväärset mõju.

Andmekaitse töögrupi õiguslik arvamus automatiseeritud otsuste osas ei anna head põhjendust, mida eeltoodud termini all võidakse mõelda. Töörühm selgitab, et kui õigusliku tagajärge ei saabu, võib otsus langeda siiski artikli 22 lõike 1 mõju alla, kui see avaldab mõju, mis on selle mõjuga võrreldes sama oluline. Märkimisväärse mõju avaldamiseks peab mõju olema rohkem, kui tavapärane ning peab olema piisavalt tähtis, et sellele tähelepanu juhtida.[136]Näiteks on selliseks mõjuks veebipõhise krediiditaotluse automaatne tagasilükkamine või veebipõhine tööle värbamine ilma inimsekkumiseta.[137]

[134] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 181.
[135] Martini, in: Paal/Pauly, DSGVO, art 22 (2017), rec. 23.
[136] Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p 10.
[137] Andmekaitse määruse preambula punkt 71.

Eelnev on siiski erinev olukorrast, kus klient ei ole laenutaotlust pangale esitanud. Samuti ei tähenda automaatse pakkumise tegemata jätmine, et hiljem esitatud laenutaotlus saaks negatiivse vastuse – nii tehakse automaatseid pakkumisi reeglina klientidele ja limiitidega, mille puhul on pank kindel, et soovib ilma täiendava analüüsita lepingu sõlmida. Seega võib eelnevast järeldada, et kui kliendile on jäetud automaatne pakkumine tegemata, on kliendil siiski võimalus esitada taotlus, mistõttu ei saa väita, et pakkumise kuvamata jätmine üksi võiks tuua kaasa õigusliku tagajärje või avaldab talle märkimisväärset mõju, sest pakkumise kuvamata jätmine ei takista kliendil panka laenutaotlust esitamast.

Andmekaitse määrus ei anna võimalust toetuda automatiseeritud otsuste tegemiseks sarnase toote/teenuse piires õigustatud huvile, kuna artikli 22 lõikes 2 nimetatud õiguslikud alused toodud otsuse tegemiseks on toodud välja kinnise loeteluna. See tähendab, et vastutava töötleja õigustatud huvi isikuandmete töötlemisel ei saa kasutada juhul, kui töötlemine langeb artikli 22 mõjualasse. Samuti ei saa otseturundustegevuse puhul alati õigustatud huvist lähtuda, vaid on vaja küsida nõusolek. Kuna aga pakkumise tegemist ja õigusliku tagajärje saabumist saab eristada, siis sarnaste toodete pakkumisi justkui õigustatud huvi alusel võib kliendile siiski kuvada, kui ta pole selleks esitanud artikli 21 kohase vastuväite.

Igal juhul tuleks sellise töötlemise korral kehtestada sobivaid kaitsemeetmeid, mis peaksid hõlmama andmesubjektile konkreetse teabe andmist ja õigust otsesele isiklikule kontaktile, õigust väljendada oma seisukohta, õigust saada selgitust otsuse kohta, mis tehti pärast sellist hindamist, ning õigust seda otsust vaidlustada.[138]

IKS § 17 lõike 1 kohaselt on keelatud andmetöötlussüsteemi poolt ilma andmesubjekti osaluseta otsuse (edaspidi *automaatne otsus*) tegemine, millega hinnatakse tema iseloomuomadusi, võimeid või muid isiksuseomadusi, kui see toob andmesubjektile kaasa õiguslikke tagajärgi või mõjutab teda muul viisil märkimisväärselt. Nii seaduse ega seletuskirjas pole täpsustatud, millisel juhul on tegemist andmesubjekti osalusega. Näiteks on leitud, et automaatsete otsuste tegemise keeld ei kehti, kui asjasse puutuv isik on selleks otsesõnu soovi avaldanud.[139] IKS-i üldine kohaldatavus ei sõltu isikuandmete töötlemise viisist (automatiseeritud või mitteautomatiseeritud). Seega IKS kohaldub kõikidele juhtudele, kui seaduses pole sätestatud teisiti.[140]

[138] Andmekaitse määruse preambula punkt 71.
[139] Justiitsministeerium on taganud isikuandmete töötlemise õiguspärasuse süsteemi loomisega, mille tulemusena töötleti välja infosüsteemide turvameetmete süsteem ISKE. ISKE ohtude kataloog. Lubamatud automaatsed otsused üksikjuhtumite kohta isikuandmete töötlemisel. https://iske.ria.ee/8_02/ISKE_ohtude_kataloog/G2/G_2.173.
[140] E.Tikk ja A. Nõmper, lk 70.

Erandina on see lubatud § 17 lõike 2 alusel lepingu sõlmimise või täitmise käigus tingimusel, et andmesubjekti taotlus rahuldatakse ning talle on jäetud vastuväite esitamise võimalus. See tähendab, et õigusvastane on olukord, kus arvuti otsustab sisestatud andmete alusel taotluse rahuldamisest keeldumise etteantud parameetrite (näiteks andmesubjekti tööviljakus, krediidivõime, usaldusväärsus, käitumine jms) järgi automaatselt ja pole ette nähtud sellise otsuse üle vaatamist.[141] Teise erandina on automaatsete otsuste tegemine lubatud seaduse alusel (IKS § 17 lg 2 p 2).

Andmekaitse määruse kohaselt on üks erinevus varasema regulatsiooniga seega, et andmesubjekti suhtes võib võtta vastu ka negatiivse otsuse, kui ta on selleks nõusoleku andnud.

2.7.2.5. Otseturundus

Eelnevalt on selgitatud, et andmekaitse määruses on peetud otseturunduslikel eesmärkidel isikuandmete töötlemise aluseks õigustatud huvi.[142] Siiski võib e-privaatsuse määrusega tulla kohustus teatud juhtudel ka otseturunduspakkumiste jaoks võtta andmesubjektilt andmekaitse määruse nõuetele vastav nõusolek. Nõusoleku selgitamise vajadus otseturunduse puhul on antud töö kontekstis väga oluline, kuna õiguskirjanduses on paljud näited toodud just otseturunduse põhjal ning neid näiteid on kasutanud ka töö autor nõusoleku tingimuste selgitamisel.

2.7.2.5.1. Otseturunduse mõiste

Enne nõusoleku vajaduse selgitamist on vaja lahti mõtestada otseturunduse mõiste. Andmekaitse määruses pole otseturunduse mõistet defineeritud ning samuti puudus definitsioon andmekaitse direktiivis. Mõiste sisustamisel saab abi aga e-privaatsuse määrusest. E-privaatsuse määruse eelnõus tähendab otseturundusteadaanne mis tahes kujul kirjaliku või suulist reklaami, mis saadetakse ühele või mitmele elektroonilise side teenuse kindlakstehtud või kindlakstehtavale lõppkasutajale, sealhulgas inimsekkumist vajavate või mittevajavate automatiseeritud numbrivalimis- ja sidesüsteemide kasutamine, elektronpost, SMS jms; (e-privaatsuse määrus art 4 lg 3 p f).

Otseturunduse all peetakse silmas kõiki tegevusi, mille abil saab kaupmees pakkuda tooteid ja teenuseid või vahendada mingeid muid sõnumeid nii olemasolevatele kui ka võimalikele klientidele posti, telefoni või muu otsest kontakti võimaldava vahendi kaudu.[143]Otseturundus

[141] Isikuandmete kaitse seaduse seletuskiri. 1026 SE, lk 21.
[142] Vt ptk 2.6.
[143] Recommendation No. R (97) 5 of the Committee of Ministersto Member States on the Protection of Personal data used for the purposes of direct marketing, p 2.

võib tähendada ka turundusinformatsiooni edastamist reklaamide kaudu, mis on kuvatud veebileheküljel või mobiilirakendustes.[144]

Täna kehtivas IKS-is pole otseturunduse mõistet defineeritud, vaid mõiste on avatud IKS-i seletuskirjas. Seaduse seletuskirjas on öeldud, et otseturunduse puhul on tegemist kommertsteadaannete saatmisega.[145] Infoühiskonna teenuse seaduse § 5 lõike 1 järgi on kommertsteadaanne igat liiki teabe edastus, mis on kavandatud otseselt või kaudselt edendama teenuse osutaja nimel kaupade või teenuste pakkumist või tõstma teenuse osutaja mainet. Seega igasugused reklaampakkumised, kus mingeid tooteid või teenuseid reklaamitakse, on sisuliselt kommertsteadaanded, sest selliste toodete reklaamimise eesmärgiks on edendada isiku kaupade või teenuste pakkumist.[146]

Otseturustuse eriliigina on nähtud ka käitumispõhise reklaami kasutamist, mis tähendab inimese veebikäitumise analüüsil põhinevat profileerimist ja tuvastatud huvide põhjal reklaami kuvamist.[147] Seega ei kuulu siia mõiste alla näiteks tänavale või mujale avalikku kohta üles pandud reklaam, mis ei ole suunatud konkreetsele isikule, vaid üldsusele.

Kuna otseturundus võib hõlmata ka automatiseeritud töötlemist, millele kohalduvad veel rangemad nõuded andmekaitse määruse artiklist 22 tulenevalt, saab autori hinnangul jagada otseturunduse mõiste kaheks. Esiteks saab otseturunduses eristada otseposti, mis hõlmavad näiteks uudiskirju, kaupmehe pakutavate toodetega, mis pole niivõrd personaliseeritud ja ei pea ilmtingimata põhinema automatiseeritud töötlusel. Teiseks saab otseposti juures eristada personaalseid pakkumisi, mis põhinevad juba kliendiandmete profileerimisel.

Näiteks saadab toidukauplus e-posti teel klientidele, kes on nõustunud pakkumiste saatmisega, iganädalasi uudiskirju soodustoodetest. Sellisel juhul on tegemist otsepostiga. Kasvavas e-poodide võrgustikus on aga toidupoel võimalik lihtsalt jälgida isikute ostukorvi sisu. Ostukorvi sisu analüüsides on kauplusel võimalik hakata tegema pakkumisi konkreetse kliendi huve ja vajadusi arvestades. Sellisel juhul on tegemist personaalsete pakkumistega, mis põhineb profileerimisel.

Available:https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=605791&SecMode=1&DocId=688244&Usage=2.

[144] Martini, in: Paal/Pauly, DSGVO, art 21 (2017), rec. 40.

[145] Isikuandmete kaitse seaduse seletuskiri. 1026 SE, lk 11.

[146] Andmekaitse Inspektsioon. Elektrooniliste kontaktandmete kasutamine otseturustuseks, lk 5. Kättesaadav: http://www.aki.ee/et/juhised.

[147] M. Mikiver. Kes on tarbija kliendiandmete peremees? Otseturustus krediidiasutuste näitel. – Juridica 2015, IV, lk 1.

Eristamine on oluline, sest kui personaalsed pakkumised põhinevad üksnes automatiseeritud töötlemisel ning pakkumise aktsepteerimisel toob see kaasa õigusliku tagajärje, on tegemist kokku automatiseeritud otsusega andmekaitse määruse artikli 22 tähenduses, mis toob kaasa teistsugused õigused ja kohustused nii andmesubjektile kui töötlejale.

2.7.2.5.2. Nõusoleku vajadus otseturunduse puhul

Nõusoleku vajadus otseturunduse puhul tuleneb e-privaatsuse määrusest. E-privaatsuse määruse artikkel 16 punkt 1 sätestab, et füüsilised või juriidilised isikud võivad kasutada elektroonilise side teenuseid, et saata otseturundusteadaandeid füüsilisest isikust lõppkasutajatele, kes on andnud selleks oma nõusoleku.

E-privaatsuse määruse kohaselt on nõusoleku vajaduse juhud ettevõtetel:

- Elektroonilise side teenuste osutajatel elektroonilise side sisu töötlemiseks (artikkel 6 lõige 3);
- Otseturunduspakkumiste saatmiseks (artikkel 16 lõige 1).

E-privaatsuse määruse artikkel 9 lõige 1 viitab, et nõusoleku nõuetele kohaldatakse andmekaitse määruse artikli 4 punktis 11 ja artiklis 7 sätestatud nõusoleku mõistet ja nõusoleku andmise tingimusi. See tähendab, et alati kui e-privaatsuse määrusega nõutakse nõusolekut, tuleb järgida andmekaitse määruses sätestatud nõusoleku nõudeid. Andmekaitse määruse nõusoleku nõudeid ei peeta täiendavateks kohustusteks, vaid pigem seadusliku töötlemise eeltingimusteks.[148] Seda põhimõtet saab kohaldada ka otseturundusinfo saatmisele.

Kui andmekaitse määrus ja IKS on sätestanud kaitse andmesubjektile kui füüsilisele isikule, siis e-privaatsuse määrus seab samasugused nõuded ka juriidilisele isikule. Nimelt näeb e-privaatsuse määruse artikkel 16 lõige 1 ette, et otseturunduspakkumiste edastamiseks elektrooniliste side kanalite kaudu on nõusolekut vaja ka juriidiliselt isikult. Elektroonilise side teenustena kanalitena loetleb e-privaatsuse määrus automatiseeritud numbrivalimis- ja sidesüsteeme, kiirsõnumirakendusi, e-posti, SMSi, MMSi, Bluetoothi või muud sarnast.[149]

Autori hinnangul ei piirdu turundusteadete edastamine üksnes eelneva loeteluga. Turundusteateid edastatakse kliendile ka siis, kui klient külastab ettevõtte kontorit. Kui klient tuleb ettevõtte kontorisse nõustamisele, siis e-privaatsuse määrus ei kohaldu, sest kontor pole elektroonilise side teenuse kanal. Samuti pole elektroonilise side kanalites välja toodud telefoni.

[148] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 5.
[149] E-privaatsuse määruse preambula punkt 33.

Seega pole autori arvates kontoris kliendile otseturundusteadete kuvamiseks ja pakkumiste tegemiseks kliendi nõusolekut vaja, mistõttu saab tugineda õigustatud huvile. Samuti võib pakkumisi saata õigustatud huvi alusel kliendi kodusele aadressile.

E-privaatsuse määrusest tuleneb lähtuvalt mõistlikkuse printiibist erand, mille kohaselt on mõistlik lubada e-posti ja SMS kontaktandmete kasutamist olemasoleva kliendisuhte kontekstis sarnaste toodete või teenuste pakkumiseks. See võimalus peaks kehtima ainult selle ettevõtte puhul, mis on omandanud elektroonilised kontaktandmed kooskõlas andmekaitse määrusega.[150] Eelnev tähendab, et lisaks saab õigustatud huvile tugineda siiski ka e-posti ja SMS-i teel turundusteadete edastamisele tingimusel, et pakkumine ei erine teenusest, mida klient on ettevõttest saanud ning kontaktandmed ning kliendi andmed on kogutud teenuse osutamise käigus.[151]

Näiteks saab arvutipood oma klientidelt oma kontaktandmeid toote müügi kontekstis ja kasutab neid kontaktandmeid tavapäraste posti teel oma sarnaste toodete turustamiseks, saates teateid uute sarnaste toodete saatmiseks. Sel juhul saab ettevõte tugineda õigustatud huvile.[152] See-eest pakkumised muude toodete kohta, mida klient pole ostnud, võivad õigustatud huvi kohta ette nähtud raamidest väljuda ning selleks on vaja kliendi nõusolekut. Samuti ei saa autori hinnangul otseturunduspakkumiste juures tugineda õigustatud huvile isikute osas, kes pole kliendid, sest andmesubjekti ja töötleja vahel puudub õigussuhe. Järelikult on mitte-klientidele pakkumiste E-privaatsuse määrus artikkel 6 punkt 3 sätestab, et elektrooniliste side teenuste turustamiseks ja lisaväärtusteenuste osutamiseks võib üldkasutatavate elektrooniliste sideteenuste osutaja töödelda lõikes 1 osutatud andmeid selliste teenuste või turustamise jaoks vajalikul määral ja vajaliku aja jooksul, kui kasutaja, kelle kohta andmeid töödeldakse, on andnud oma eelneva nõusoleku. Kasutajatele ja abonentidele antakse võimalus oma liiklusandmete töötlemiseks antud nõusolek igal ajal tühistada. Abonent on füüsiline või juriidiline isik, kes sõlminud üldkasutatavate elektrooniliste sideteenuste osutajaga lepingu teenuste kasutamiseks.[153] Seega teatud liiki teenuste puhul võib nõusolekut vaja abonendilt ning teistel juhtudel võib olla otstarbekas nõusolek küsida otse kasutajalt.

[150] E-privaatsuse määruse preambula punkt 33.
[151] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p 59.
[152] *Ibid*.
[153] Õiguskantsleri märgukiri e-postile edastatava reklaami kohta, lk 6. Kättesaadav: http://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_margukiri_e-posti_aadressile_edastatav_reklaam.pdf.

Eestis hakati nö rämpsposti õiguslikult reguleerima infoühiskonna teenuse seaduse jõustumisega 2004. aastal,[154] mis oli suunatud elektroonilise kaubanduse direktiivi 2000/31[155] üle võtmisele. Esimesed aastad seaduse kohaldamise praktikas näitasid, et ei Eestis ega Euroopa liidu riikides rämpsposti hulk ei vähenenud.[156]

Infoühiskonna teenuse seaduse § 5 käsitleb kommertsteadaannet kui igasugust teavet, mis on kavandatud otseselt või kaudselt edendama majandus- või kutsetegevuses osaleva isiku nimel tema kaupade või teenuste pakkumist või tõstma sellise isiku mainet. Seega mahub selle mõiste alla ka otseturundusinfo, kuna eesmärk on edendada juriidilise isiku kaupade või teenuste pakkumist.

Varasemalt tulenes infoühiskonna teenuse seaduse §-st 6 õigus esitada e-posti aadressile kommertsteadaannet üksnes adressaadi eelnevalt antud nõusolekul. Infoühiskonna teenuse seaduse § 6 lõige 2 pani teenuse osutajale kohustuse ka nõusolek või keeldumine registreerida ning lõike 3 kohaselt tuli teenuse osutajal ka nõusoleku olemasolu tõendada. Seega oli e-privaatsuse direktiivi eeskujul kehtestatud nn *opt-in*-süsteem. Infoühiskonna teenuse seaduse reguleerimisala ja subjektide ring on oluliselt kitsam kui e-privaatsuse direktiivi artikkel 13 kohaldumisala, mistõttu ei täitnud Eesti Euroopa liidu õigusega kehtestatud kohustusi. Sellest tulenevalt tekkis vajadus asendada olemasolevad sätted sätetega, mis korrektselt harmoniseerivad e-privaatsuse artikli 13 nõudeid. Sellega tunnistati 2010. aastal infoühiskonna teenuse seaduse § 6 kehtetuks, kuna Eesti õigusesse poldud üldistest *opt-in* reeglitest tehtavaid erandeid[157] ning elektrooniliste kontaktandmete kasutamist otseturustuseks hakati reguleerima elektroonilise side seaduses.

Täna kehtiva IKS § 12 lõikes 5 on antud andmesubjektile õigus keelata igal ajal teda käsitlevate andmete töötlemine tarbijaharjumuste uurimiseks või otseturustamiseks ja andmete üleandmine kolmandatele isikutele, kes soovivad neid kasutada tarbijaharjumuste uurimiseks või otseturustamiseks. Viidatud sättest ei tulene otseselt, et pakkumiste saatmiseks on vaja nõusolekut, vaid see tuleneb Elektroonilise side seaduse § 103^1 lõikest 1, mille kohaselt on füüsilisest isikust sideteenuse kasutaja või kliendi elektrooniliste kontaktandmete kasutamine otseturustuseks on lubatud üksnes tema eelneval nõusolekul. Nõusolek peab vastama isikuandmete kaitse seaduse §-s 12 sätestatud tingimustele.

[154] Infoühiskonna teenuse seadus. Vastu võetud 14.04.2004. RT I 2004, 29, 191.
[155] Euroopa parlamendi ja nõukogu 8. Juuni 2000. Aasta direktiiv 2000/31/EÜ, infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul – EÜT 178, 17.07.2001, lk 1.
[156] E. Tikk ja A. Nõmper, lk 138.
[157] Seletuskiri elektroonilise side seaduse ja infoühiskonna teenuse seaduse muutmise seaduse eelnõu juurde, lk 1-2.

Juriidilise isiku puhul on ESS § 103[1] lõike 2 alusel tema elektrooniliste kontaktandmete kasutamine otseturustuseks lubatud, kui kontaktandmete kasutamisel iga kord on jäetud võimalus keelata oma kontaktandmete selline kasutamine, ehk rakendatakse nn *opt-out* põhimõtet ehk kinnitava teksti juures eelnevalt tehtud märge, mis tähendab, et seni polnud juriidilise isiku puhul kohustust nõusolekut võtta. Üheks muutuseks, mis e-privaatsuse määrusega kaasneb, on kohustus võtta nõusolek otseturunduse jaoks ka juriidilistelt isikutelt.

Kehtivas IKS-is ette nähtud, et otseturundusinfo saatmiseks tuleb saada kliendi nõusolek (IKS § 12 lõige 5). Seejuures pole eristatud otseturunduses erinevaid olukordi, mille kohaselt saab erinevatele eesmärkidele kohaldada erinevat õigusliku alust (st. nõusolekut või õigustatud huvi). Järelikult tuleb ettevõtetel hakata eristama, milline olukord langeb õigustatud huvi alla ning milliste turunduspakkumiste saatmisel on vaja andmesubjekti nõusolekut. Esmalt tuleb selgitada kõik otseturundustegevusega seonduvad töötlemise protsessid ning seejärel saab iga töötlemise puhul eraldi hinnata, mille alla kõnealusel eesmärgil töötlemine võib minna.

2.7.3. Uues isikuandmete kaitse seaduse eelnõus toodud isikuandmete töötlemise erijuhud

2018. aasta isikuandmete kaitse seaduse eelnõu käsitleb erijuhtudena peamiselt olukordi, mil isikuandmete töötlemine võib toimuda ilma nõusolekuta. Nõusoleku vajadus on erinevalt andmekaitse määrusest seatud isikuandmete töötlemisele pärast andmesubjekti surma. Nimelt näeb 2018. a. IKS-i eelnõu § 9 lõige 2 ette, et andmesubjekti isikuandmeid võib töödelda pärast tema surma pärija nõusoleku alusel. Nõusolekut pole vaja, kui töödeldakse üksnes nime, sugu, sünni- ja surmaaega ning surma fakti.

Andmekaitse määrus on jätnud võimaluse liikmesriikidel otsustada, lisaks eelnevatele olukordadele, mõnede erandite üle, mil töötlemine võib toimuda ilma nõusolekuta. Neid erandeid saab lähemalt vaadata uue isikuandmete kaitse regulatsiooni eelnõust. 2018. a. IKS-i eelnõu sätestab erandid, millest tulenevalt isikuandmete töötlemine võib toimuda ilma andmesubjekti nõusolekuta. Näiteks sätestatakse erandid ajakirjanduse (2018. a. IKS-i eelnõu § 4), kunstilise ja kirjandusliku eneseväljenduse (2018. a. IKS-i eelnõu § 5), teadusuuringu või riikliku statistika vajaduseks (2018. a. IKS-i eelnõu § 6) ning avalikes huvides arhiveerimise eesmärgil töötlemiseks (2018. a. IKS-i eelnõu § 7).

2018. a. IKS-i eelnõu § 4 lõige 1 sätestab ühe võimalusena, et ilma andmesubjekti nõusolekuta võib isikuandmeid töödelda ajakirjanduslikul eesmärgil, kui selleks on ülekaalukas avalik huvi ning see on kooskõlas ajakirjanduseetika põhimõtetega.

Õigus liikmesriigile erandi ettenägemiseks tuleb andmekaitse määruse artikli 85 lõikest 1, mille kohaselt liikmesriigid ühitavad õigusaktiga isikuandmete töötlemise ajakirjanduslikel eesmärkidel. Lõikest 2 tuleneb, et selle tarbeks võib näha ette muuhulgas vabastusi andmekaitse määruse II-st peatükist, kui need on vajalikud, et ühitada õigus isikuandmete kaitsele sõna- ja teabevabadusega. Nimelt on nii rahvusvahelises õiguses kui ka Eesti põhiseaduse §-s 45 tunnustatud ajakirjandusvabadust. See tähendab, et riik ei tohi ajakirjandusvabadusse sekkuda, samas on riigil kohustus tagada põhivabaduse toimimine õigusraamistiku ja õiguskaitsevahendite abil.[158] Seega on tegemist vabastusega andmekaitse määruse II peatüki § 6 lõikest 1 punktis a, mille puhul töötlemiseks on vaja nõusolekut.

Ka kehtivas IKS-is on täna selline erand olemas, mille kohaselt andmesubjekti nõusolekuta või töödelda ja avalikustada meedias, kui selleks on ülekaalukas avalik huvi ning see on kooskõlas ajakirjanduseetika üldpõhimõtetega (2008 a. IKS § 11 lg 2). Seega ei muutu andmekaitse määrusega isikuandmete töötlemise põhimõte, mis vajalik ajakirjanduslikul eesmärgil.

Teise erandina, mis erasektorit puudutab, on isikuandmete töötlemine kunstilise ja kirjandusliku eneseväljenduse tarbeks. 2018. a. IKS-i eelnõu § 5 lõige 1 sätestab, et isikuandmeid võib ilma andmesubjekti nõusolekuta töödelda kunstilise ja kirjandusliku eneseväljenduse eesmärgil, eelkõige avalikustada, kui see ei kahjusta ülemäära andmesubjekti õigusi.

Õiguslik alus liikmesriigile täiendavate meetmete sätestamiseks tuleneb samuti andmekaitse määruse artikli 85 lõikest 1, mille kohaselt liikmesriigid ühitavad õigusaktiga isikuandmete töötlemise kunstilise või kirjandusliku eneseväljenduse tarbeks. Sarnaselt eelmise näitega on tegemist siinkohal samuti vabastusega nõusoleku küsimise nõudest.

Tänases IKS-is sellist õigust eraldi reguleeritud pole, nagu oli eelmises näites ajakirjandusvabaduse puhul. Seega tuleb kuni uue IKS-i jõustumiseni võtta kõnealusel eesmärgil andmesubjektilt nõusolek vastavalt 2008. a. IKS § 10 lõikele 1.

Samuti võib IKS-i kohaselt isikuandmeid töödelda andmesubjekti nõusolekuta teadusuuringu või riikliku statistika vajadusteks (2018. a. IKS-i eelnõu § 16) ning selline õigus on liikmesriikidele otsustamiseks jäetud andmekaitse määruse artikliga 89. Samast sättest tuleneb ka õigus liikmesriikidel otsustada nõusoleku vajaduse üle avalikes huvides arhiveerimise eesmärgil. Ka kehtivas IKS-is nähakse ette võimalus ilma andmesubjekti nõusolekuta

[158] Isikuandmete kaitse seaduse eelnõu seletuskiri. 06.11.2017, lk 9.

isikuandmete töötlemine teadusuuringu või riikliku statistika eesmärgil (IKS § 15), samas puudus erand arhiveerimise eesmärgil töötlemiseks.

Eelnevast nähtub, et 2018. a. IKS-i eelnõu mitmeid võimalusi olukordade jaoks, mil nõusolekut pole vaja, sealhulgas on uueks võimaluseks ilma nõusolekuta töödelda kunstilise ja kirjandusliku eneseväljenduse eesmärgil ning arhiveerimise eesmärgil.

3. TINGIMUSED KEHTIVALE NÕUSOLEKULE

Andmekaitse määruse kohaselt saab isikuandmete töötlemisel andmesubjekti nõusolekule tugineda üksnes siis, kui see on võetud kõiki andmekaitse üldmääruse nõudeid järgides. Kui isikuandmete töötlemine põhineb nõusolekul, mille suhtes pole kõiki andmekaitse määruse nõuded järgitud, pole sellise nõusoleku alusel isikuandmete töötlemine kehtiv.[159] Seega on äärmiselt oluline selgitada, millised tingimused andmekaitse määrus nõusolekule seab ning kuidas praktikas neid nõudeid täita.

Andmekaitse määruse artikkel 4 punkt 11 sätestab, et andmesubjekti nõusolek on vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega. Vabatahtlikkus, konkreetsus, teadlikkus ja ühemõtteline tahteavaldus pole Euroopa Liidu tasandil isikuandmete kaitses uued kriteeriumid,[160] mistõttu saab nende tingimuste tõlgendamisel arvesse võtta ka varasemaid arvamusi, mis põhinesid andmekaitse direktiivil.

3.1. Vabatahtlikkus

3.1.1. Valikuvabadus

Nõusoleku alusel isikuandmete töötlemise üheks esimeseks eeltingimuseks on andmekaitse määruse artikli 4 punkti 11 kohaselt vabatahtlikkus. Vabatahtlikkuse hindamisel tuleb arvesse võtta erinevaid kriteeriumeid, mida läbi analüüsides jõuab järelduseni, kas vabatahtlikkuse element on olemas.

Esimeseks eelduseks on andmesubjekti tegelik valiku - ja kontrollivabadus.[161] Nõusolek on vabatahtlik üksnes juhul, kui andmesubjektil on reaalne valikuvõimalus ning teda ei ähvarda pettuse, hirmutamise või sundimise oht või olulised negatiivsed tagajärjed mittenõustumise korral.[162] See tähendab ühtlasi, et nõusoleku andmiseks ei tohi andmesubjektile survet avaldada.

Praktikas võivad ettevõtted isikuandmete töötlemiseks nõusoleku küsimisel korraldada loosimisi, pakkuda klientidele soodustusi või muid hüvesid, et meelitada andmesubjekte

[159] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 4.
[160] Andmekaitse direktiivi artikli 2 punkt h sätestab, et nõusolek on iga vabatahtlik, konkreetne ja teadlik tahteavaldus, millega andmesubjekt annab nõusoleku töödelda tema kohta käivaid andmeid. Andmekaitse direktiivi artikli 7 punktist a tuleneb, et isikuandmeid võib töödelda ainult juhul, kui andmesubjekt on selleks andnud oma ühemõttelise nõusoleku.
[161] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 6.
[162] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 12-13.

valikuid tegema. See tekitab küsimusi, millistel tingimustel ib täiendavate hüvede pakkumine lubatud, et hüve pakkumine ei mõjutaks andmesubjekti valiku- ja kontrollivabadust.

Ebakohaseks surveks või mõjutuseks ei tohiks pidada üksikisikule erinevate hüvede pakkumist täiendava töötlemisega nõustumiseks (näiteks tasu vähendamine või muu kasuliku lisavõimaluse või teenuse pakkumine). Sellisteks täiendavateks hüvedeks, millega andmesubjekti ei survestata, võivad olla näiteks loosimises osalemised ja soodushinnaga täiendava teenuse pakkumine.[163] Seega ei tohiks ettevõtetel täielikult välistada isikuandmete töötlemiseks nõusoleku küsimisel täiendavate hüvede pakkumist. Kui aga auhinda ei loosita kõikide jah/ei vastanute vahel, vaid ainult nende vahel, kes nõustusid pakkumiste saatmisega, võib olla autori hinnangul tegemist siiski andmesubjektide survestamisega, mis mõjutab vabatahtlikkuse olemasolu. Seega peab eristama, kas hüve pakkumine on seotud valiku tegemisega sõltumata nõusoleku andmisest või on hüve seotud konkreetselt nõusoleku andmisega.

Vabatahtlikkuse juures on ka oluliseks aspektiks, et isikuandmete töötlemisega mittenõustumisel ei kaasneks negatiivseid tagajärgi.[164] Vastutav töötleja peab tõestama, et nõusoleku tagasivõtmine ei põhjusta andmesubjektile kulusid ning nõusoleku tagasivõtmisel ei saabu tema jaoks ebasoodsamat olukorda kui see, milles ta oli enne.

Kui vastutav töötleja suudab näidata, et teenuse pakkumine on võimalik viisil, mis sisaldab võimalust nõusolekut tagasi võtta ilma negatiivsete tagajärgedeta, on nõusolek antud vabalt. Siin pole oluline negatiivse tagajärje mainimine, vaid oluline on küsimus, kas tagajärg ka reaalselt saabub või mitte.[165] Sellest tulenevalt ei ole vabatahtlikkuse elemendi olemasolu küsimuse all juhul, kui andmesubjekt üksnes arvab, et töötlemisega võib saabuda negatiivne tagajärg.[166] Seega ei saa käsitleda vabatahtlikuna sellist nõusolekut, mis on antud eeldusel, et nõusoleku andmisest keeldumisel ähvardatakse halvema teenuse pakkumisega.

[163] Centre for Information Policy Leadership. Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Consent", p 5.
[164] ITGP Privacy Team. EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide. Ely: IT Governance Publishing 2017, p 207.
[165] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 13.
[166] Vahel võidakse reisijale jätta mulje, et kehaskanneri läbimine on vabatahtlik. Samas võivad reisijad karta, et sellega mitte nõustumine võib tekitada lennujaama töötajates kahtlust ning nad peavad läbima hoopis füüsilise läbiotsimise. Füüsilise läbiotsimise vältimiseks, nõustuvad nad kehaskännimisega. Õiguskirjanduses leiti, et selline nõusolek pole vabatahtlik, mis tähendab, et vabatahtlikkust võiks mõjutada ainuüksi andmesubjekti arvamus. Fundamental Rights Agency, p 55.

Autori hinnangul on eelmise kahe näite puhul tekkinud olukord, kus ühest küljest võib andmesubjektile öelda, et andmesubjekt võib valiku andmata jätmisel jääda ilma positiivsest tagajärjest. Samas ei tohi nõusoleku andmata jätmise tõttu saabuda negatiivne tagajärg.

Eelnev ei tähenda siiski, et nõusolek ei saa kunagi olla kehtiv tingimustes, kus mittenõustumisel võib olla negatiivseid tagajärgi. Kui klient ei nõustu kliendikaardi väljastamisega ning ei saa seetõttu allahindlust, pole mittenõustumise tagajärjed andmesubjekti vaba valiku välistamiseks piisavalt tõsised ning puudub ka alluvussuhe.[167]

Eelnevast saab järeldada, kui e-poest tellimuse esitamisel on tellimuse juures poe poolt ette kirjutatud kinnitustekst, mille kohaselt klient annab tellimuse esitamisega poele nõusoleku pakkumiste saatmiseks ning kinnitustekst on seejuures kohustuslik element, pole samuti tegemist vabatahtliku nõusolekuga. Põhjus seisneb selles, et kliendil puudub võimalus poe poolt koostatud kinnitusteksti mõjutada ning nõusolekut mitte anda. Vastutav töötleja võib väita, et tema organisatsioon pakub andmesubjektidele tõelist valikuvõimalust, kui neile pakutakse võimalust valida teenuste vahel, mis sisaldab ühelt poolt isikuandmete kasutamist nõusolekul ja seejuures pakkuda samaväärset teenust, mis ei vaja nõusolekut andmete kasutamiseks. Senikaua, kuni täiendav teenus ei mõjuta lepingu täitmist, tähendab see tingimuslikkuse puudumist.[168] Eelnev näitab, et vastutav töötleja peab olema eriti ettevaatlik, kui ta küsib lepingu sõlmimise juures nõusolekut lepinguga seotud isikuandmete töötlemiseks.

Saksa õiguses on vabatahtlikkuse elementi selgitatud ka nii, et kui ettevõttel on monopol, siis ei või ettevõte muuta nõusolekut lepingu täitmisest sõltuvaks, sest sellisel juhul puudub isikul võrdväärne juurdepääs samaväärsele teenusele ilma nõusoleku andmiseta.[169] Monopoli seisundis ettevõtte poolt nõusoleku nõudmisel pole tegemist vabatahtliku nõusolekuga.

Teisalt tekib küsimus, et kui andmesubjekt keeldub nõusolekut andmast, siis kas ettevõte tohib kord kuus paluda kliendil oma valikuid, mis puudutab nõusoleku andmist, uuendada. Sellise tegutsemise vajadus võib olla tingitud sellest, et inimesed võivad oma varasemaid seisukohti muuta. Ühendkuningriikides on järelevalveasutus leidnud, et klientide puhul, kes pole otsustanud, kas lubada turundusinfo saatmine või mitte, ei tohiks saada e-kirju, kus palutakse valikuid uuendada, kuna andmesubjekt pole selliste kirjade saamisega nõustunud.[170] Sama

[167] Fundamental Rights Agency, p 56.
[168] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 10.
[169] Sec. 28 para 3.b BDSG. A. Bussche; P. Voigt. Data protection in Germany: including EU General Data Protection Regulation. Berlin: Springer 2018, p 12.
[170] The Information Commissioner. Monetary penalty notice to Honda Motor Europe Limited t/a Honda (U.K.). London: 20.03.2017. Available: https://ico.org.uk/media/action-weve-taken/mpns/2013732/mpn-honda-europe-20170320.pdf.

kehtib ka nende puhul, kes on selgelt väljendanud soovi mitte saada turundusinfot.[171] Järelikult saab ettevõte paluda oma valikuid uuendada üksnes nendel klientidel, kes on nõustunud sellise e-kirja saamisega.

IKS § 12 lõikest 1 tuleneb, et andmesubjekti tahteavaldus, millega ta lubab oma isikuandmeid töödelda kehtib üksnes juhul, kui see tugineb andmesubjekti vabal tahtel. Seega on ka IKS-is sõnaselgelt vabatahtlikkuse element sätestatud ning andmesubjekt saab valida, kas anda töötlemiseks nõusolek või mitte. Eestis pole aga õiguskirjanduses ega kohtupraktikas vabatahtlikkuse tähendust põhjalikult selgitatud. Küll on aga leitud, sarnaselt andmekaitse määruses kehtestatud põhimõttega, et nõusoleku andmisel ei tohi isik olla sundolukorras.[172] See tähendab, et IKS-i rakendamisel on lähtutud sarnastest põhimõtetest, mis tulenevad andmekaitse määrusest nõusoleku nõuete põhjendamisel.

Vabatahtlikkust võib tuletada ka tehingu mõistest. Eelnevalt on tuvastatud, et nõusolek on tehing.[173] Eesti õiguse kohaselt ei tohi tehing olla tehtud eksimuse, pettuse, ähvarduse või vägivalla mõjul (TsÜS § 90 lg 1). Selge on see, et kui esineb pettus, ähvardus või vägivald, pole nõusolek antud vabatahtlikult ning isik saab tehingu tühistada. Samas kui nõusolek on antud ähvarduse tagajärjel, saab vabatahtlikkuse puudumisel tugineda tsiviilseadustiku üldosa seaduse alusel tehingu tühistamisel IKS-ile, mille kohaselt nõusolek pole kehtivalt antud, kui puudub vaba tahe.

Lisaks tuleb vaadata ka eksimuse aspekti. Eksimus on ebaõige ettekujutus tegelikest asjaoludest (TsÜS § 92 lg 1). Eksimuse olukord võib autori hinnangul tekkida pigem juhul, kui nõusolek pole väljendatud selgesõnaliselt või nõusoleku küsimisel pole esitatud andmesubjektile vajalikku teavet ja see on loonud ebaõige ettekujutuse tegelikkusest. See ei tähenda aga seda, et nõusolek poleks antud vabatahtlikult, vaid pigem on tagajärg asjaolule, kui ettevõte on jätnud nõusoleku juures teabe esitamise kohustuse täitmata. Samas pole ei praegu ega tulevikus vaja eksimuse asjaolule nõusoleku tagasivõtmiseks tugineda, kuna nii IKS kui andmekaitse määrus on andnud selleks eraldi alused, mis on TsÜS-i regulatsioonist ka märksa laiema rakendusalaga.

Samuti tuleb andmekaitse määruse artikkel 7 lõike 4 kohaselt selle hindamisel, kas nõusolek anti vabatahtlikult, võimalikult suurel määral võtta arvesse asjaolu, kas lepingu täitmise,

[171] The Information Commissioner. Monetary penalty notice to Moneysupermarket.com Ltd. London: 17.07.2017. Available: https://ico.org.uk/media/action-weve-taken/mpns/2014482/mpn-moneysupermarket-ltd-20170720.pdf.
[172] A. Henberg, lk 562.
[173] Vt. peatükki 2.7.2.1.

sealhulgas teenuse osutamise tingimuseks on muu hulgas seatud nõusoleku andmine isikuandmete töötlemiseks, mis ei ole lepingu täitmiseks vajalik.

Lepingu täitmiseks vajaliku töötlemisega on tegemist juhul, kui töötdeldakse andmesubjekti aadressi, et kaupleja saaks veebis ostetud kaupu kätte toimetada või pangal maksete hõlbustamiseks töödelda krediitkaardi andmeid.[174] Seega paneb andmekaitse määrus ettevõtetele kohustuse selgelt eristada töötlemise eesmärgid ja õiguslikud alused ning küsida nõusolek ainult nende juhtumite jaoks, mis ei sobi muu õigusliku aluse kohaselt töötlemiseks, et olla kooskõlas andmekaitse määruse artikkel 7 lõikega 4. Kui täna on IKS-i kohaselt nõusoleku alusel töötlemine prioriteetne, siis andmekaitse määrus muudab seda põhimõtet ning enne nõusoleku võtmist tuleks kontrollida, ega ei sobi mingi muu alus isikuandmete töötlemiseks. Seeläbi omab tingimuslikkuse puudumise nõude sätestamine olulist sisulist mõju isikuandmete töötlemisele Eestis, võrreldes täna kehtiva olukorraga.

3.1.2. Jaotatavuse põhimõte

Lisaks valikuvabadusele tuleb vaadata vabatahtlikkuse juures ka nö osadeks jaotatavuse põhimõtet.[175] Jaotatavuse põhimõte tuleneb sellest, et alati ei piirdu teenuse pakkumine ühe eesmärgiga. Teenus võib hõlmata mitut töötlemist enam kui ühe eesmärgi jaoks. Sellistel juhtudel peaks andmesubjektidel olema vabadus valida, millise isikuandmete töötlemise eesmärgiga nad nõustuvad, selle asemel, et nõustuda töötlemisega seotud kogumiga. Andmekaitse määruse alusel võib ettevõte küsida ühe teenuse pakkumiseks korraga mitut nõusolekut.[176] Seega puudub nõusoleku piirang, kui palju võib andmesubjektilt erinevaid nõusolekuid küsida.

Andmekaitse määruse preambula punktis 43 selgitatakse, et nõusolekut ei loeta vabatahtlikuks, kui ei ole võimalik anda erinevatele isikuandmete töötlemise toimingutele eraldi nõusolekut. Eelnev tähendab, et eesmärgid tuleb eraldada ja nõusolek tuleb saada eraldi iga töötlemise eesmärgi jaoks. Seega kui vastutav töötleja on mitu töötlemise eesmärki ühendanud ja ei ole püüdnud otsida eraldi nõusolekut iga eesmärgi jaoks, siis puudub vabatahtlikkus.

Teisalt sätestab määruses preambula punktis 32, et nõusolek peaks hõlmama kõiki samal eesmärgil või samadel eesmärkidel tehtavaid isikuandmete töötlemise toiminguid. Seega

[174] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 9.
[175] Ing. k. granularity.
[176] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 11.

kooskõlas artikli 5 lõike 1 punktiga b ja preambula punktiga 32 võib nõusolek hõlmata erinevaid toiminguid, kui need toimingud teenivad sama eesmärki.[177]

Õiguskirjanduses on leitud, et erinevate eesmärkidega on tegemist juhul, kui müüja on ühes nõusolekus küsinud oma klientidelt nõusolekut kasutada nende andmeid, et saata neile turundusteateid e-posti teel ning samuti, et jagada kliendi andmeid ka oma partneritele nende poolsete pakkumiste saatmiseks.[178] Järelikult määruse nõuetele vastavuseks peaks olema klientidel võimalus anda nõusolek müüjale tema poolt pakkumiste edastamiseks ning eraldi anda nõusolek partneritele pakkumiste edastamiseks.

Autori hinnangul on eri eesmärkidega tegemist siiski juhul, kui ettevõte jagab andmeid kolmandatele ettevõtetele, kes ei kuulu nõusoleku küsinud ettevõttega ühte kontserni.

Ühe probleemina nähakse andmekaitse töögrupi arvamuses seisukohta, mille kohaselt töörühm leiab, et ettevõtte kontsernisiseselt andmete jagamise ühe eesmärgi alla paigutamise puhul pole tegemist kehtiva nõusolekuga.[179] Nimelt nähakse kontserni siseses jagamises eraldi eesmärki. Andmekaitse töögrupi seisukohaga pole aga kõik nõus. Õigusmaastikul leitakse vastuargumendina, et tegemist on ühe töötlemise toiminguga, mitte eraldi eesmärgiga, mistõttu eraldi nõusolek pole vajalik. Iga väiksema eesmärgi jaoks nõusoleku küsimine võib tekitada olukorra, kus tekib nõusolekust nö ülekoormatus. Selle tagajärjeks on oht, et nõusolek kaotab oma mõtte, kuna inimesed enam ei keskendu pidevate nõusolekute küsimiste tõttu nende lugemisele ja seega nõusolekut ei anna. Samuti võib kontsernisisene andmete jagamise keeld tuua ka negatiivse mõju majandusele.[180] Ka autori hinnangul võiks nõusoleku küsimine kontserni jaoks olla kooskõlas määruse nõuetega, kui see info on nõusoleku juures ka selgelt välja toodud.

Samas on ka andmekaiste töörühm ise nentinud, et olukord, kus andmesubjektile esitatakse juba liiga palju erinevaid nõusoleku taotlusi, võib kaasa tuua selle, et neid taotlusi ei loeta enam läbi. Lahendusena saaks teha veebilehitsejas eraldi lehekülje seadete haldamiseks, seejuures peab selline nõusolekute haldamise leht olema siiski kooskõlas andmekaitse määruse nõuetega.[181] Üheks võimaluseks oleks, ettevõttel endal luua veebileheküljele nõusolekute haldamise osa.

[177] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 12.
[178] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 11.
[179] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 12-13.
[180] Centre for Information Policy Leadership. Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Consent", p 7.
[181] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 18.

Teine võimalus oleks pakkuda ettevõtetele teenust, kus eri ettevõtted ostavad nõuetele vastava nõusoleku küsimise teenust ning vastu pakutakse veebilehekülge, kus neid saab hallata.

Kui töötlemise eesmärgid on seotud, kontseptuaalselt sarnased või tehniliselt üksteisest sõltuvad, on kliendile selgem, informatiivsem ja mõistlikum, kui isik esitab nõusoleku mitmel eesmärgil koos. Selline lähenemisviis on rohkem kooskõlas andmekaitse määruse kasutajaspetsiifilise tõlgendusega ehk nõusoleku küsimine peab olema selge, kokkuvõtlik ja mitte põhjendamatult häiriv.[182] Seega tuleks jaotatavuse põhimõttele läheneda paindlikumalt.

Lisaks küsimusele, kas erinevate ettevõtete vahel on kontserni siseselt andmete jagamiseks vaja eraldi nõusolekut, tekib küsimus sisu eristamises, milleks nõusolek antakse. Näiteks, kas otseturunduspakkumisi saab kajastada justkui ühtse töötlemise eesmärgina, kui pakkumised võivad hõlmata nii uudiskirju toodetest ja teenustest, kui ka näiteks kutseid kliendiüritustele uute kaupade tutvustamiseks. Lähtudes eelnevalt selgitatud jaotatavuse põhimõttest, tuleks kliendi kurnamise vältimiseks autori hinnangul jaatada seda, et nii uudiskirjad kui kutsed üritustele mahuvad otseturunduse mõiste alla ning otseturunduse mõistet ei pea nii detailselt lahti mõtestama. Vastasel juhul tooks see kaasa olukorra, et kliendile antakse ette paber, mis on täis kirjutatud erinevaid nõusoleku taotlusi. Sellisel juhul on tõenäoline, et klient ei soovi neid üldse läbi vaadata või annab ilma sisule keskendumata kõigele nõusoleku. Nõusoleku valimatul andmisel võib see pärssida andmesubjekti õiguseid ning nagu eelnevalt leitud, sellest valimatul keeldumisel aga majandust.

Eelnev tähendab siiski ka seda, et kui ettevõte on nõusoleku küsimisel eristanud erinevaid pakutavaid teenuseid ning klient on nõustunud üksnes ühe teenuse kohta pakkumiste saatmisega, siis ei või ettevõte siiski saata pakkumisi teiste teenuste kohta.

Ka andmekaitse määruse preambula punktis 50 märgitakse, et isikuandmete töötlemine muudel eesmärkidel kui need, milleks isikuandmed algselt koguti, peaks olema lubatud üksnes juhul, kui töötlemine on kooskõlas eesmärkidega, mille jaoks isikuandmed algselt koguti. Seega on määrus siiski jätnud võimaluse eesmärkide vahetumisel lubada isikuandmete töötlemise jätkamist, kui uued eesmärgid on kooskõlas eelmistega.

Isikuandmete töötlejal on oluline jälgida, et nõusoleku küsimisel oleks koheselt kõik töötlemise eesmärgid välja toodud. Vastasel juhul võib see kaasa tuua olukorra, kus isik võtab nõusoleku tagasi, aga tegelikult peaks töötlemine jätkuma. Näiteks kasutab isik terviserakendust, milles

[182] Centre for Information Policy Leadership. Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Consent", p 7.

saab sisestada vererõhu näitu, kaalu jms andmeid ning kasutaja on andnud rakenduse loojale neid andmeid töödelda terviseseisu kuvamiseks. Kui aga nõusolek tagasi võtta, siis see ei tähenda, et kasutaja ei sooviks, et varem avaldatud andmed koheselt kustuks.[183] Sellisel juhul töötlejale on oluline rakenduses välja tuua, et nõusolek hõlmab ka andmete säilitamist. Vastasel korral nõusolekut tagasi võttes ei tohiks enam isikuandmeid terviserakenduses säilitada.

Tänases IKS § 12 lõikes 1 nähakse ette võimalus anda nõusolek osaliselt ja tingimuslikult. Osaline nõusolek tähendab, et andmesubjekt võib anda nõusoleku oma andmete töötlemiseks üksnes ühel eesmärgil mitmest või lubada andmeid üle anda vaid teatud isikutele või nende kategooriatele. Seega andmete töötleja võib küsida nõusoleku üheks eesmärgiks, aga andmesubjektil on võimalus vastata sellele osalise nõusolekuga. [184] Samas ei näe andmekaitse määrus ette otseselt võimalust anda nõusolek üksnes ühele osale.

Täna pole ka Andmekaitse Inspektsioon oma juhiste kaudu IKS-i tõlgendades asunud seisukohale, et andmete töötlemise eesmärke tuleks nii täpselt eristada. Seega võib IKS-i kohaselt täna olla kehtiv nõusolek, millega klient nõustub üldiselt otseturundusinfo saatmisega ning ka grupiüleselt, kui seejuures on selgitatud, kellele andmeid jagatakse ja mis eeesmärgil. Samas ei tulene Eesti õiguses selgelt, et nõusolekut on vaja iga eesmärgi jaoks, mis tähendab, et andmekaitse määrus näeb ette selgemad juhised.

Seega puudub kehtiva IKS-i alusel kohustus eesmärke eraldada, vaid andmesubjektil endal on võimalus eesmärke eristada ja anda nõusolek üksnes osaliselt. Samas võib praktikas siiski olla juba täna ettevõtteid, kes küsivad iga eesmärgi jaoks eraldi nõusolekut. Nende jaoks seega eesmärkide jaotatavuse põhimõtte osas midagi ei muutu.

Andmekaitse määrus ei sätesta sõnaselgelt õigust andmesubjektil endal anda nõusolekut osaliselt. Praktikas koostab ettevõte nõusoleku vormi ette ning andmesubjektil on võimalus otsustada, kas nõustub nõusoleku küsimise vormi kinnitamast või mitte. Olukorras, kus kliendil palutakse valida, millise kanali teel pakkumisi soovib saada ja ta valib ainult ühe mitmest, võib tegemist olla osaliselt nõusoleku andmisega. Kui andmesubjekt soovib nõusoleku vormist kõrvale kalduda ja saavutada hoopis muu kokkulepe, pole see andmekaitse määruse nõuete alusel küll sõnaselgelt keelatud, kuid siin tekib kahtlus, kas ettevõttel on võimalik erandit hallata. Kui see võimalus on olemas, siis tingimusliku nõusoleku andmine on aktsepteeritav

[183] Centre for Information Policy Leadership. Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Consent", p 18.
[184] Isikuandmete kaitse seaduse seletuskiri. 1026 SE. Justiitsministeerium, lk 13.

juhul, kui ettevõte sellega nõustub. Vastasel juhul saab ettevõte käsitleda seda kui nõusoleku mitteandmist, kui ta ei nõustunud töötlemise eesmärkidega.

Andmekaitse määruse alusel tuleb selgeks teha, millised eesmärgid teenivad sama eesmärki ja millised mitte. Samas pole andmekaitse määrus ise eesmärkide eristamise kohta väga häid juhiseid andnud. Seega on ettevõtetel oht hinnata ekslikult osad isikuandmete töötlemise toimingud sama eesmärgi alla, kuid järelevalve käigus võib selguda, et tegemist oli hoopis eraldi eesmärkidega ning see võib kaasa tuua trahvi.

2018. a. IKS-i eelnõus ei jaotatavuse põhimõtet ei reguleerita, mistõttu ei peatu autor uuel IKS-il pikemalt.

3.2. Konkreetsus

Andmekaitse määruse artikli 6 lõige 1 punkt a sätestab, et andmesubjekti nõusolek tuleb anda ühel või mitmel konkreetsel eesmärgil, mis tähendab, et andmesubjektil on võimalus iga eesmärgi puhul kaaluda nõusoleku andmist. Konkreetsuse nõude eesmärk on tagada andmesubjektile teatav kontroll ja läbipaistvus. Konkreetsuse nõude juures on oluline, et andmesubjekt saaks anda igale töötlemise toimingule eraldi nõusoleku, et tagada kooskõla ka nõusoleku vabatahtlikkuse tingimusega[185] ning eriti jaotatavuse põhimõttega. Konkreetsuse nõue käib käsikäes ka nõusoleku eesmärgi kohta antava teabe kvaliteediga.[186]

Konkreetsuse nõude täitmiseks peaksid vastutavad töötlejad esitama konkreetse teabe eraldi iga nõusoleku taotluse kohta, mis käsitlevad iga eesmärgi jaoks töödeldavaid andmeid, et andmesubjektid saaksid teadlikuks nende erinevate valikute mõjust.[187] See on seotud ka teadlikkuse põhimõttega, mida käsitletakse peatükis 3.3. Aktsepteeritav pole nõusoleku küsimine üldistel või ebamääraselt sõnastatud eesmärkidel, jättes töötlemise täpse eesmärki täpsustamata.[188] Seega on konkreetsuse kriteeriumi täitmiseks vajalik detailselt sõnastatud eesmärk. Detailsuse aste töötlemise eesmärkidest teavitamisel varieerub iga üksikjuhtumi põhiselt. Selle välja selgitamisel tuleb lähtuda töötlemise kontekstist, andmesubjekti mõistlikest ootustest. Näiteks on leitud, et mida rohkem on andmesubjekte mõjutatud, seda selgem peab eesmärk olema. Samuti peab rohkem detailidesse laskuma, kui töötlemine ületab seda eesmärki, mis tavaliselt on kõnealuses kontekstis.[189]

[185] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 12.
[186] Fundamental Rights Agency, p 57.
[187] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 13.
[188] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 17.
[189] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 89.

Samuti saab konkreetsuse all mõista seda, et nõusolek peab olema arusaadav ehk see peaks selgelt ja täpselt ära näitama andmetöötluse ulatuse ja tagajärjed, et andmesubjekt saaks nõusoleku anda vastavalt töötlemise ulatusele.[190]

Töötlemise eesmärkide selgitamisel on muuhulgas oluline, et andmete töötleja kaaluks läbi, kas kogutav info on ka tegelikult eesmärgi saavutamiseks vajalik. See tuleneb minimaalsuse põhimõttest (IKS § 6 p 3). Minimaalsuse põhimõtte eesmärgiks pole mitte vähendada andmete töötlemise toiminguid, vaid töötlemiseks kogutavate andmete mahtu.[191]

Konkreetsuse nõuet on selgitatud ka kohtupraktikas. *Deutsche Telekom AG* vs Saksamaa kohtuasjas käsitles Euroopa Kohus küsimust, kas telekommunikatsiooniettevõtja, kellel oli vaja edastada kasutajate isikuandmeid e-privaatsuse direktiivi artikli 12 alusel[192], pidi paluma nõusoleku üle kinnitamist, kuna andmete saaja polnud nõusoleku andmisel teada. Euroopa Kohus leidis, et nõusolek anti üksnes eesmärgiga töötlemisega nõustuda, seega polnud andmesubjektil võimalik valida, kellele neid avaldada, mistõttu pole artikli 12 alusel uut nõusolekut vaja, kuna selle sätte eesmärk on küsida nõusolek üksnes üldkasutatavas kataloogis avaldamiseks.[193] Seega olukorras, kus nõusoleku vajadus tuleb mõnest muust Euroopa Liidu õigusaktist, tuleb vaadata täpselt eesmärki, mille jaoks õigusakt nõusolekut küsima kohustab. Siin on Euroopa Kohus selgitanud, et nõusoleku küsimisel ei pea seaduse sätte mõttest kaugemale minema.

Isikuandmete saajate nimekirjaga seondub ka küsimus, kas nimekiri võib töötlemise ajal muutuda ning kas selle muutumisel on vaja saada kliendilt uus nõusolek. Kuna nimekiri pole nõusoleku osa, vaid täidab informeerimiskohustust, siis võib järeldada, et nimekirja muutumisel uut nõusolekut pole vaja küsida. Küll võib aga nõusoleku saajal tekkida kohustus andmesubjekti nimekirja muudatusest teavitada.

Samas on õiguskirjanduses selgitatud, et kui muudetud eesmärk on esialgses eesmärgis enam-vähem kajastatud või seda võiks eeldada loogilise järgneva etapina, võib see siiski olla sobiv kasutamine ja ühilduda küsitud nõusoleku eesmärgiga.[194] Järelikult tuleb hinnata, mida mõistlik

[190] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 17.
[191] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 90.
[192] E-privaatsuse direktiiv artikkel 12 lõige 2 sätestab: "Liikmesriigid tagavad, et abonentidele antakse võimalus otsustada, kas nad soovivad lasta oma isikuandmeid kanda üldkasutatavasse kataloogi, ja kui nad seda soovivad, siis millises ulatuses, kuivõrd sellised andmed on olulised kataloogi koostaja määratletud otstarbe seisukohast, ning selliseid andmeid kontrollida, parandada ja kustutada."
[193] EKo, 05.05.2011, C-53/09, *Deutsche Telekom AG* vs. *Saksamaa*, p 61.
[194] Article 29 Data Protection Working Party. Opinion 03/2013, p. 24.

inimene sellises olukorras eeldaks. Kui mõistlik inimene sellist kasutust eeldaks, siis võib see eesmärgi alla mahtuda.

IKS ei käsitle konkreetsuse põhimõtet ning samuti pole konkreetsuse põhimõtet käsitletud ka Andmekaitse Inspektsiooni juhistes ega õiguskirjanduses. Seega saab järeldada, et konkreetsuse põhimõte on ettevõtete jaoks Eesti õigusmaastikul uueks kriteeriumiks. Ettevõtted peavad nõusoleku küsimisel seega arvestama, kui täpne peab nõusolek olema ning milliste eesmärkidega seotud. 2018. a. IKS nõusoleku konkreetsust ei reguleeri, mistõttu tuleb lähtuda määrusest.

3.3. Teadlikkus

3.3.1. Edastamist vajav teave

Andmekaitse määruse artikli 4 punkti 11 kohaselt on järgmine oluline aspekt andmesubjekti nõusoleku küsimisel teadlik tahteavaldus. Selge viide teadliku nõusoleku andmise kohustusele tuleneb ka andmekaitse määruse preambula punktist 42, mis selgitab, et teadliku nõusoleku andmiseks peaks andmesubjekt olema teadlik vähemalt sellest, kes on vastutav töötleja ja milleks kavatsetakse isikuandmeid töödelda. See tähendab, et andmesubjektil peab olema enne otsuse tegemist piisavalt teavet. Teabe esitamise kohustust ei täideta aga mitte andmesubjekti taotlusel, vaid vastutav töötleja peab seda täitma proaktiivselt, sõltumata sellest, kas andmesubjekt tunneb kõnealuse teabe vastu huvi või mitte.[195] Teabe piisavuse üle saab otsustada aga ainult iga üksikjuhtumi puhul eraldi.

Andmekaitse töörühm on oma viimases nõusoleku nõudeid selgitavas juhises leidnud, et andmekaitse määrus tugevdab informeerimise kohustust. Andmekaitse määruse artikli 5 lõike 1 alusel on läbipaistvuse nõue üks põhiprintsiipe, mis on tihedalt seotud õigluse ja seaduslikkuse põhimõtetega. Andmesubjektidele teabe andmine enne nende nõusoleku saamist on oluline teadlike otsuste tegemiseks. Lisaks peavad nad mõistma, millega nad nõustuvad ja andmesubjektid peavad saama kasutada oma õigust nõusolekut tagasi võtta. Juhul, kui vastutav töötleja ei anna juurdepääsetavat teavet, ei saa andmekaitse subjekt omada kontrolli nõusolekute üle, mis võib muuta nõusoleku alusel töötlemise kehtetuks.[196]

Andmesubjekti on vaja teavitada teatavatest elementidest, mis on valiku tegemiseks äärmiselt olulised. Andmekaitse määrusest tuleneb informeerimise kohustus artiklitest 12-14. Siin peab andmesubjekti informeerimisel eristama kahte olukorda. Esiteks, andmekaitse määruse artikkel

[195] Fundamental Rights Agency, p 94.
[196] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 13.

13 lõiked 1 ja 2 eristavad teavet, mis tuleb andmesubjektile edastada andmete kogumise hetkel ning teiseks tuleb hiljemalt ühe kuu jooksul edastada ka muu oluline teave.

Andmete kogumise hetkel tuleb artikli 13 kohaselt andmesubjektile esitada:

1) vastutava töötleja (ja asjakohasel juhul andmekaitseametniku) kontaktandmed;
2) töötlemise eesmärk ja õiguslik alus;
3) kui isikuandmete töötlemine põhineb artikli 6 lõike 1 punktil f, siis teave vastutava töötleja või kolmanda isiku õigustatud huvide kohta;
4) asjakohasel juhul teave isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta;
5) asjakohasel juhul teave selle kohta, et vastutav töötleja kavatseb edastada isikuandmed kolmandas riigis asuvale vastuvõtjale või rahvusvahelisele organisatsioonile.

Teadliku nõusoleku andmiseks peaks andmesubjekt olema teadlik vähemalt sellest, kes on vastutav töötleja ja milleks kavatsetakse isikuandmeid töödelda.[197] Seega peab vastutav töötleja tagama, et nõusolek antakse teabe alusel, mis võimaldab andmesubjektil lihtsalt tuvastada, kes on vastutav töötleja ja mõista, millega ta nõustub. Vastutav töötleja peab selgelt kirjeldama andmetöötluse eesmärki, milleks nõusolekut taotletakse. Töötlejaid ei pea nimetama nõusolekus, kuid andmekaitse määruse artiklite 13 ja 14 järgimiseks peavad vastutavad töötlejad esitama täieliku nimekirja andmete saajatest.[198] Võttes eelneva kokku, on kõige olulisem teave alati info sellest kes, milleks ja mille alusel töötleb.

Vastutavad töötlejad peaksid esitama koos iga nõusoleku taotlusega info, mis käsitleb iga eesmärgi jaoks eraldi töödeldavaid andmeid, et andmesubjektid saaksid teadlikuks nende erinevate valikute mõjust. Sellega võimaldatakse andmesubjektidel anda teadlik nõusolek.[199]

Hiljemalt ühe kuu jooksul tuleb andmesubjektile andmekaitse määrus artikli 13 lõike 2 alusel edastada info isikuandmete säilitamisest, andmesubjekti õigustest, kaebuse esitamise õigusest, teave selle kohta, kas andmete esitamine on vajalik seaduse või lepingu täitmise jaoks ning andmete mitte-esitamise tagajärgedest ning teave automaatsete otsuste kohta. Andmekaitse määrus ei keela infot esitamast ka kohe. Kui andmed ei pärine andmesubjektilt, tuleb asjakohasel juhul teavitada isikut ka õigustatud huvist ning andmete päritoluallika kohta.

[197] Andmekaitse määruse preambula punkt 42.
[198] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 14.
[199] *Ibid*, p 13.

Kui ettevõte küsib nõusolekuid kahe erineva eesmärgi jaoks, peab nendest mõlemast isikuandmete töötlemise eesmärgist andmesubjekti teavitama. Näiteks kolmandatele isikutele pakkumiste saatmiseks ning käitumispõhise reklaami pakkumiseks.[200]

Lisaks tulevad mõned täiendavad nõuded veel ka teistest sätetest. Nimelt sätestab andmekaitse määruse artikkel 7 lõige 3 kohustuse isikut teavitada tema õigusest nõusolek igal ajal tagasi võtta. Automatiseeritud töötluse puhul on vajalik teave andmete automatiseeritud otsuste, sealhulgas profiilianalüüsi kohta (andmekaitse määruse art 13 lg 2 p f). Andmekaitse töörühm märgib, et sõltuvalt asjaoludest ja kontekstist võib olla vaja rohkem teavet, et andmesubjektil oleks võimalik töötlemistoimingutest tegelikult aru saada.[201] Eelnev olukord võib tekkida juhul, kui isikuandmete töötlemine on tavapärasest mahukam või ka siis, kui töödeldakse isikuandmeid, mille töötlemise tagajärgi tavaisik ei pruugi mõista (näiteks geneetiliste andmete töötlemine). Seega eeltoodud info pole lõplik.

Kui isikuandmeid töötleb mitu töötlejat (kaasvastutavad töötlejad), tuleb kõikide töötlejate kontaktandmed andmesubjektile välja tuua, kui mõlemad töötlejad tuginevad nõusolekule.[202]

IKS-is on samuti ette nähtud kohustuslik teave, mida töötleja peab nõusolekus esitama. IKS § 12 lõige 1 sätestab, et nõusolekus peavad olema selgelt määratletud andmed, mille töötlemiseks luba antakse, andmete töötlemise eesmärk ning isikud, kellele andmete edastamine on lubatud, samuti andmete kolmandatele isikutele edastamise tingimused ning andmesubjekti õigused tema isikuandmete edasise töötlemise osas.

Andmesubjekti õigused on sätestatud IKS-i kolmandas peatükis. Selle kohaselt tuleb teavitada andmesubjekti veel õigusest saada teavet, õigusest nõuda töötlemise lõpetamist, parandamist, sulgemist ja kustutamist, õigusest pöörduda Andmekaitse Inspektsiooni ja kohtu poole ning õigusest nõuda kahju hüvitamist. Seega on nõusoleku teadlikkuse kriteerium kajastatud ka kehtivas IKS-is. Kehtiv regulatsioon erineb aga andmekaitse määrusest selles osas, et määrus eristab nõusolekut ja nõusoleku küsimiseks esitatavat teavet aga IKS-i järgi moodustab kohustuslik informatsioon justkui nõusoleku osa. Kui nõusolekust oli mingi oluline teave välja jäänud, võis sellega IKS-i kohaselt saabuda kohe nõusoleku tühisus. Samas see ei tähenda, et andmekaitse määruse alusel olulise teabe välja toomata jätmine, ei võiks tuua nõusoleku tühisust kaasa.

[200] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 97.
[201] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 14.
[202] *Ibid*.

Lisaks tulevad nõuded kohustusliku teabe osas ka IKS § 12 lõikest 3, millest tulenevalt peab ettevõte enne teatavaks tegema isikuandmete töötleja või tema esindaja nime ning isikuandmete töötleja aadressi ja muud kontaktandmed. Kui isikuandmeid töötlevad vastutav töötleja ja volitatud töötleja, siis tehakse teatavaks või kättesaadavaks vastutava ja volitatud töötleja või nende esindajate nimed ning vastutava ja volitatud töötleja aadressid ja muud kontaktandmed.

Eestis täna kehtiva regulatsiooni tõlgendamisel on Andmekaitse Inspektsioon viidanud sellele, et andmesubjekti nõusolek peab olema informeeritud. Informeerituse eesmärk on tagada, et andmesubjekt saab teabest aru, mis võimaldab tal teha informeeritud otsuseid. See tähendab, et andmesubjektile esitatav teave peab olema lihtsalt mõistetava keelekasutusega.[203] Eelnevast saab järeldada, et informeeritus ja teadlikkus on printsiibis sama tähendusega.

Võrreldes kehtiva IKSi-ga tuleb andmesubjekti täiendavalt teavitada näiteks töötleja ja andmekaitseametniku kontaktandmetest, isikuandmete säilitamise ajavahemikust või säilitamise kriteeriumitest, töötleja õigustatud huvist ning õigusest võtta nõusolek tagasi.

Samas sõltub osa kohustusliku teabe esitamise vajaduse mahust konkreetsest olukorrast, kuna artiklite 13 ja 14 kohaselt ei tule kogu teavet esitada iga kord, vaid üksnes asjakohasel juhul. Seega suureneb andmekaiste määrusega esitatava teabe maht sõltuvalt sellest, kas tegemist on erandjuhtumiga, mil andmekaitse määrus näeb ette täiendava teabe esitamise kohustuse. Lisaks eristab andmekaitse määrus erinevad teabe esitamise nõuded sõltuvalt sellest, kas andmed on kogutud andmesubjektilt või saadud mujalt. Näiteks, kui andmed pole kogutud andmesubjektilt, tuleb esitada teave selle kohta, kust andmed pärinevad (andmekaitse määruse art 12 lg 2 p f). Teabe loetelu on aga väga pikk ning ettevõtetel võib olla keeruline jälgida, millise isikuandmete töötlemise juhtumiga on tegemist ning sellest tulenevalt jälgida, milline on edastamiseks vajalik teave. See võib kaasa tuua olukorra, kus igaks juhuks esitakse andmesubjektile ka erandolukorda puudutav teave, koormates seeläbi andmesubjekti mahukate teabelehtedega.

Uus isikuandmete kaitse seaduse eelnõu eristab teavet, mis tuleb andmesubjektile kättesaadavaks teha veebilehel või muul andmesubjektile kergesti juurdepääsetavas asukohas teabest, mis tuleb anda siis, kui seaduses on sätestatud kohustus teavitada andmesubjekti tema isikuandmete töötlemisest.[204]

[203] Andmekaitse inspektsioon. Informeeritud nõusolek isikuandmete töötlemiseks. 01.03.2013. Kättesaadav: http://www.aki.ee/et/mida-peab-teadma-isikuandmete-tootlemisest/informeeritud-nousolek-isikuandmete-tootlemiseks.
[204] 2018 a. isikuandmete kaitse seaduse eelnõu, § 25 ja § 26.

Kohustusliku informatsiooni, millest andmesubjekti peab isikuandmete töötlemiseks nõusoleku küsimisel teavitama, on üle võetud andmekaitse määrusest ka uude IKS-i. 2018. a. IKS-i eelnõu kohaselt tuleb teha kättesaadavaks teave, mis puudutab töötlemise eesmärki, andmete parandamise, kustutamise või piiramise õigusi ja õiguste teostamise korda, vastutava töötleja ning andmekaitseametniku nime ja kontaktandmeid, Andmekaitse Inspektsiooni kontaktandmeid ja kaebuse esitamise õigust (2018. a. IKS-i eelnõu § 25). Andmesubjekti teavitamisel seadusest tuleneva kohustuse korral tuleb lisaks eelnevale teabele esitada veel töötlemise õiguslik alus, andmete säilitamise tähtaeg, vastuvõtjate kategooriad, kellele on lubatud edastada isikuandmeid ning muu asjakohane teave (2018. a. IKS-i eelnõu § 26). Sellega ei muutu põhimõte, et üldiselt tuleb teavitada sellest, et kes, milleks ja mille alusel isikuandmeid töötleb. 2018. a. IKS-is on §-des 25 ja 26 kokku võetud ka muu andmekaitse määrusest tulenev kohustuslik informatsioon, millest andmesubjekti peab teavitama, nagu näiteks erinevad õigused (parandamine, kustutamine, piiramine), säilitamise aeg, vastuvõtjate kategooriad. Kuna andmekaitse määrus on otsekohalduva iseloomuga, on see regulatsioon siiski rohkem deklaratiivne.

Sõltuvalt olukorrast, tuleb ettevõtjatel seega hoolega jälgida, millist teavet on kõnealuses situatsioonis vaja kliendile enne nõusoleku andmist edastada, kuna isikuandmete senise regulatsiooniga võrreldes on andmekaitse määrus suurendanud kohustust vajaliku teabe osas, mis tuleb andmesubjektile nõusoleku küsimisel edastada. Kuna 2018. a. IKS-i eelnõus on võetud esitatav teave üle andmekaitse määrusest, saab võtta muutuse hindamisel arvesse eelnevalt tehtud võrdlust kehtiva IKS-i ja andmekaitse määruse vahel.

3.3.2. Teabe edastamise viis

3.3.2.1. Teabele esitatavad formaalsed nõuded

Andmekaitse määrus näeb andmesubjektile esitatavale teabe ette formaalsed nõuded. Andmekaitse määruse artikli 12 kohaselt peab vastutav töötleja võtma asjakohased meetmed, et esitada andmesubjektile artiklites 13 ja 14 osutatud teave ning teavitada teda artiklite 15–22 ja 34 kohaselt isikuandmete töötlemisest kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt.

Kokkuvõtlikkus tähendab, et teave peab olema korrektne ja sisu osas terviklik.[205] Järelikult tuleb vältida ebavajalikku informatsiooni.

[205] Pauly in: Paal/Pauly, DSGVO, Art 12. (2017), rec. 28.

Teabe selguse nõue hõlmab endas ka selge ja lihtsa keele nõuet. See tähendab, et teave tuleb esitada lihtsas keeles, arusaadavalt sh ilma erikeele kasutuseta ja teabe hulgast peab oluline teave välja paistma. Teabe esitamise viisi puhul on oluline ka jälgida, et ka keskmine kasutaja seda mõistaks. Samuti ei tohiks esitatav teave jätta ruumi erinevate tõlgenduste jaoks. [206] Järelikult ei tohiks kohustusliku teabe esitamisel kasutada keerulisi termineid ning tuleb vältida erialakeelt ja kantseliiti.

Selge ja lihtsa keele puhul tuleks samuti vältida topelt eituse kasutamist.[207] Kui kliendil tuleb valida mitme nõusoleku vahel, tuleks nende nõusoleku vormide vahel hoida sarnast joont nii keeleliselt kui struktuuriliselt. [208]

Teadliku nõusoleku andmiseks on vajalik, et kohustuslikust infost saaks aru ka võõramaalane. Kui ettevõttel pole koheselt andmesubjekti poolt valdavas keeles nõusoleku vormi kliendile anda, peab ettevõte leidma muu viisi, kuidas kliendile nõusoleku sisu arusaadavalt selgeks teha. Vastasel juhul ei saa väita, et klient oleks andnud teadliku nõusoleku. Samas võib selline nõue põhjustada probleeme, kuna näiteks veebikaubamajal või muul teenusepakkujal võib olla väga keeruline tuvastada, mis keelt räägib isik, kes tema veebilehel nt Eesti IP-aadressilt käib. Seetõttu tuleb autori hinnangul asuda seisukohale, et kui veebileht kuvab kohustusliku info vastavas riigis enamlevinud keeltes (Eesti puhul eelkõige eesti ja vene keeles), on ta enda kohustused teabe andmisel täitnud.

Arusaadavuse nõue tähendab, et seda peaks mõistma sihtgrupi keskmine liige. See tähendab, et vastutav töötleja peab kõigepealt kindlaks määrama kavandatava sihtgrupi ja kindlaks määrama keskmise liikme mõistmise taseme. Andmekaitse töögrupi arvamuse kohaselt vastutavad töötlejad ei peaks mitte ainult esitama ettenähtud teavet artiklite 13 ja 14 alusel, vaid ka eraldi selgitama üheselt mõistetavas keeles, millised on kõige olulisemad töötlemise tagajärjed. [209] Sihtgrupi määramisel tuleks lähtuda vastavalt mõistlikkuse põhimõttele sellest, et kellele see toode või teenus suunatud.

Isegi siis, kui nõusoleku peab andma vanem, peab kohustuslik informatsioon olema arusaadav ka lapsele.[210] See tähendab, et vajalik teave tuleb edastada nii lihtsalt, et lapsel oleks võimalik

[206] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 20.
[207] Information Commissioner's office. Consultation: GDPR consent guidance, p 30.
[208] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 14.
[209] Article 29 Data Protection Working Party. Guidelines on Transparency Under Regulation 2016/679. WP 260. Brussels: 2017, p 8. Available: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615250.
[210] ITGP Privacy Team, p 219.

sellest aru saada. Samas pole autori hinnangul mõistlik, et teave peaks olema arusaadav ka 7-aastasele lapsele selliste teenuste puhul, mis pole eelkõige lastele mõeldud.

Eelnevast saab järeldada, et mida keerukam andmetöötlus, seda raskem on tavalisel inimesel mõista ja jälgida kõiki andmetöötluse elemente. Keeruka andmetöötluse korral on ka andmete töötlejal raskem ka tõendada, et nõusolek on saadud informatsiooni alusel, mis on esitatud konkreetselt ja arusaadavalt.[211] Seega on andmete töötlejal kohustus edastada vajalik info võimalikult lihtsalt aga samas ka nii, et kajastatud oleks kogu oluline info. Samuti aitab tihti keerulise andmetöötluse kliendile lihtsalt selgitamine ettevõttel läbi mõelda, kas andmetöötlus sellises mahus ja sellisel kujul on ikka vajalik.

Eesti õiguskirjanduses pole teabe esitamise nõudeid nii põhjalikult lahti selgitatud. Andmekaitse Inspektsioon on selgitanud, et andmesubjektile esitatav teave peab olema lihtsalt mõistetava keelekasutusega. Lisaks on Inspektsioon juhtinud tähelepanu, et ka erivajadustega inimesed peavad nõusoleku sisust aru saama. [212] Seega sätestab andmekaiste määrus teabele esitatud nõuded, mida Eesti õiguskorras pole seaduse tasandil varasemalt reguleeritud.

Vaadates andmekaitse määruses sätestatud rangeid formaalseid nõudeid teabe esitamisele, võib ettevõtetel olla keeruline kõiki nõudeid järgida. Kuigi osad nõuded võivad olla sellised, mille peale võiks ka mõistlikult ettevõtted ise tulla, siis võttes arvesse, et nõuetega mittevastavuses olemine võib kaasa tuua suure rahatrahvi (andmekaitse määruse art 83 lg 5 p b), ei saa ettevõtted endale sellist riski lubada. Järelikult suureneb teabele esitatava nõuete järgimise kohustus.

3.3.2.2. Teabe kajastamine koos nõusolekuga vs privaatsuspoliitikas

Järgmine element on teabe lihtsa kättesaadavuse nõue, mis tuleneb andmekaitse määruse artiklist 12. See põhimõte tähendab, et andmesubjekt ei peaks eraldi teavet otsima, vaid ta peaks kohe nõusoleku taotluse juures nägema, kuidas teabele juurde pääseb. [213] Teave peab olema selgelt nähtav, sh mõistlikus suuruses kirjastiiliga, esile tõstetud ja kõikehõlmav.[214]

Praktikas tihtipeale esitatakse kohustuslik teave koos nõusoleku küsimise vormiga, mida määrus ei keela. Nii nagu puudub andmekaitse määruses vorminõue nõusolekule, puudub see ka vajaliku informatsiooni edastamisele. Seega võib teavet esitada peale kirjalike võimaluste ka suuliselt, näiteks klienditeenindaja kaudu või näidata kliendile tutvustavat videot. Samas ei

[211] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 20.
[212] Andmekaitse inspektsioon. Informeeritud nõusolek isikuandmete töötlemiseks. 01.03.2013. Kättesaadav: http://www.aki.ee/et/mida-peab-teadma-isikuandmete-tootlemisest/informeeritud-nousolek-isikuandmete-tootlemiseks.
[213] Article 29 Data Protection Working Party. Guidelines on Transparency Under Regulation 2016/679, p 8.
[214] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 20.

tohi nõusoleku vormi enda juures siiski olla puudu vajalik info, mis aitaks isikul otsustada, kas nõusolekut anda.[215] Seega peab nõusoleku enda vormi juures olema siiski teave selle kohta, kes ja mis eesmärgil tahab isikuandmeid töödelda ning teave andmesubjekti õigusest nõusolek igal ajal tagasi võtta.

Probleemi on nähtud nõusoleku küsimisel e-kaubanduses, kuna siin võib olla oht, et andmesubjekt pole täielikult informeeritud või ei saa tegelikult aru, milleks ta nõusoleku annab. Seega kui andmesubjekt vajutab internetis kauba ostmiseks või teenuse kasutamiseks nupule "nõustun tingimustega", võib tema nõusolek olla nõuetele mittevastav, kui eelnevalt esitatud tingimused on liiga pikad ning on leheküljel peidetud mitme lingi taha, mistõttu puudus andmesubjektil mõistlik võimalus nendega enne nõustumist tutvuda. Andmekaitse määruse nõuetele vastavuseks peaks seega pikkade tingimustega olema enne aktsepteerimist võimalik reaalselt tutvuda.[216] See tähendab, kui kliendile kuvatakse e-kaubanduse portaalis nõusoleku küsimise vorm tingimustega nõustumiseks ja teenuse kasutamisega jätkamiseks, peab nõusoleku vormis olema juures link tingimustele või olema aken, kus on tingimused avatud ning mida klient saab läbi lehitseda. Kõige turvalisem viis tagada, et klient ka need tingimused läbi lehitseks, on lisada nõusoleku nupp tingimuste lõppu.

Samas viitab autori praktiline kogemus sellele, et reeglina ei loeta veebilehtedel kasutatavaid tingimusi läbi ka juhul, kui nende läbi lehitsemine on võimalik koheselt ja nõusoleku nupp on alles tingimuste lõpus. Seetõttu võib arvata, et selliste nõuete esitamine on kõigest teadliku nõusoleku näitemäng.

Andmekaitse määrus ei sätesta eraldi nõudeid nõusoleku küsimiseks veebis.[217] Samas peaks siiski iga veebisaiti haldav ettevõte, kes töötleb isikuandmeid, avaldama veebisaidil privaatsuspoliitika. Privaatsuspoliitika link peaks olema igal veebileheküljel olema selgelt nähtav ning sellele peaks olema viidatud üldkasutatava termini abil (nt privaatsus, privaatsuspoliitika või andmekaitse teatis). Mobiilirakenduse installimisel ei tohiks selline teave kunagi olla rohkem kui kahe kliki kaugusel. Üldiselt tähendab see seda, et rakendustes sageli kasutatavad menüüfunktsioonid peaksid alati sisaldama valikut "Privaatsus" või "Andmekaitse".[218] Selle lehe alt peaks samuti olema võimalik klientidel oma nõusoleku valikuid hallata.[219]

[215] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 14.
[216] C. Kuner. European Data Privacy Law and Online Business. London: Oxford University Press, 2003, p 68.
[217] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 93.
[218] Article 29 Data Protection Working Party. Guidelines on Transparency Under Regulation 2016/679, p 8.
[219] Information Commissioner's office. Consultation: GDPR consent guidance, p 35.

Privaatsuspoliitika kasutamisel tuleks jälgida, et vastutavad töötlejad ei kasutaks liiga pikki ja keerulisi privaatsuspoliitikaid. Privaatsuspoliitika esitamine on siiski üks tõhusamaid teabe edasi andmise viise. Samas tuleb arvestada ka sellega, et kohustuslik teave oleks kättesaadav ka neile, kes internetti ei kasuta.[220]

Samas ei pruugi elektroonilises vormis, nagu näiteks veebipõhises privaatsuspoliitikas, esitatud teabe edastamine olla asjakohane, kui isikul ei ole veebilehele juurdepääsu. Sellistel juhtudel tuleks kaaluda sobivaid alternatiivseid lisavõimalusi, näiteks pakkudes kliendile privaatsuspoliitikat paberkandjal.[221]

Vastavalt preambula punktile 32 peab nõusoleku taotlus olema selge ja kokkuvõtlik, kui andmesubjekti nõusolek tuleb anda pärast elektroonilise taotluse esitamist. Andmekaitse töörühm järeldab, et seega ei saa nõusolek olla üksnes üks punkt muude tingimuste hulgast. Kuna täna saab lepinguid sõlmida ka mobiili vahendusel, annab töörühm juhised, et nõusoleku küsimisel ja teabe edastamisel saab siiski arvesse võtta kasutajamugavust ja toote kujundust ning esitada informatsiooni etapiliselt (ing. k. *present in a layered way*).[222]

Etapiliselt informatsiooni esitamine tähendab seda, et esimeses vaates kuvatakse andmesubjektile nö kliendisõbralik versioon, mille juures on link detailsemale töötlemise kirjeldusele.[223] Ehk teave esitatakse lühiülevaates, mille kõrval saab tutvuda ka mahukama versiooniga. Näiteks on kõigepealt lühidalt ja lihtsalt kirjeldatud töötlemise eesmärgid ja muu vajalik info ning teine vaade suunab juba isikuandmete töötlemise põhimõtetele, kus on eesmärgid täpsemalt lahti kirjeldatud.

Lisaks ei või informatsioon, mis on vajalik informeeritud otsuste langetamiseks selle üle, kas anda nõusolek või mitte, olla peidetud lepingu blanketiga juurde lisatud tüüptingimustes.[224] Kui nõusoleku taotlus on ebamäärane või seda on raske mõista, siis on see kehtetu.[225] Sellest saab järeldada, et kui juba nõusoleku andmiseks vajalik informatsioon ei või olla peidetud tüüptingimustes, ei või ka nõusolek ise olla võetud tüüptingimustes.

Eesti kehtiv isikukaitse regulatsioon näeb ette, et kui nõusolek antakse koos teise tahteavaldusega, peab isiku nõusolek olema selgelt eristatav (IKS § 12 lg 2). Sätte eesmärk on vältida olukorda, kus isik, arvates, et ta kirjutab alla vaid võlaõiguslikele tingimustele, mida

[220] Fundamental Rights Agency, p 97.
[221] Article 29 Data Protection Working Party. Guidelines on Transparency Under Regulation 2016/679, p 11.
[222] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 15.
[223] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 90.
[224] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 14.
[225] Information Commissioner's office. Consultation: GDPR consent guidance, p 21.

talle on juba selgitatud ja millega ta on nõustunud, kirjutab enda teadmata muuhulgas alla ka isikuandmete töötlemise nõusolekule.[226]

Kehtivas IKS-is on täna põhimõte, mille kohaselt nõusolek ei pea olema eraldi dokumendis. Samas kui nõusolek on paigutatud tüüptingimustesse, ilma et see oleks kujunduslikult selgelt eristatav ning ilma et selle kohta oleks võimalik eraldiseisvat nõusolekut anda, ei ole täidetud ei vabatahtlikkuse ega konkreetsuse kriteeriumid. Seega on juba regulatsiooni kehtivuse ajal Andmekaitse Inspektsioon leidnud, et tüüptingimustes nõusoleku võtmine ei vasta nõusoleku tingimustele.[227] Samas on õiguskantsler andnud hinnangu, et tüüptingimustes nõusoleku regulatsioon ei ole vastuolus IKS-iga, kui see on kooskõlas andmekaitse direktiiviga.[228]

Lisaks on Eestis tüüptingimustes andmesubjektilt nõusoleku võtmine saanud õiguskirjanduses ka palju kriitikat. Pankadele ette heidetud andmetöötlust, millele alus leitakse rohketes panga poolt sätestatud tüüptingimustes. On leitud, et andmetöötlus panga enda kehtestatud reeglite alusel ei saa olla seaduslikuks aluseks ning andmesubjektil on igal ajal õigus keelduda isikuandmete avaldamisest, kui isikuandmete nõudmisel ei suudeta esitada seaduslikku alust andmete töötlemiseks.[229] Autori hinnangul saab KAS § 89 lõike 2^2 grammatilisest tõlgendamisest järeldada, kui tüüptingimustes ei selgitata, et tegemist on nõusolekuga, siis ei saa pangad KAS-i erisättele nõusolekut võtmisel tugineda.

Töörühm on leidnud, et kehtiv ja informeeritud nõusolek saab eksisteerida ka juhul, kui nõusoleku saamise protsessis ei mainita kõiki artiklite 13 ja/või 14 kohustuslike osi. Siiski tuleb kohustuslik teave tuua sellisel juhul välja teistes kohtades nagu näiteks ettevõtte privaatsuspoliitikas.[230] Seega pole kohustusliku esitatava informatsiooni hulk nõusoleku juures nii suur, kui esmapilgul tunduda võib.

Eeltoodud põhimõttest saab järeldada, et kui kogu info ei mahu nõusoleku kohustusliku teabe nimekirja, siis võib viidata ka üldiselt privaatsuspoliitikale. Seega kui andmeid jagatakse terve kontserni ettevõtetega, võib terve kontserni ettevõtte nimede välja toomise asemel öelda üksnes, et andmeid jagatakse ettevõtte kontserniga. Täpsem info peab aga sel juhul olemas olema privaatsuspoliitikas. Siiski tuleb informeerimise kohustust arvesse võttes andmesubjektile

[226] Isikuandmete kaitse seaduse seletuskiri. 1026 SE, lk 13.
[227] Andmekaitse Inspektsioon. Pankade seire seoses isikuandmete töötlemisega nõusoleku alusel ja lepingu täitmiseks. Isikuandmete kaitse seaduse täitmise seire. Tallinn: 2013, lk 2. Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Pankade_seire2013.pdf.
[228] Õiguskantsleri märgukiri KindlTS § 14^2 lg 2 ja KAS § 89 lg 2^2 ja 2^3 põhiseaduspärasuse kohta. 26.02.2014. Kättesaadav: http://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_oigus_votta_nousolek_isikuandmete_tootlemiseks_tuuptingimustes.pdf
[229] M. Männiko, lk 162.
[230] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 15.

viidata, kust ta võiks leida informatsiooni, kellega tema andmeid jagatakse. Näiteks sobiks, kui nimekiri asub isikuandmete töötlemise põhimõtetes, millele on lepingus selge viide ning millega lepingu alusel klient kohustub enne allkirjastamist tutvuma.

Eesti õiguses on tänane seadus ja praktika soodustanud samuti privaatsuspoliitikate kasutamist. Näiteks on paljudel suurettevõtetel (pangad, telekomi ettevõtted) veebilehekülgedel üleval privaatsuspoliitikad, kus selgitatakse, milliseid andmeid ja mis eesmärgil töödeldakse.[231]

Ka 2018. a. IKS-i eelnõu sätestab konkreetselt loa esitada osa kliendile kohustuslikust teabest veebileheküljel (2018. a. IKS-i eelnõu § 25). Siiski vastavalt eelmises peatükis selgitatule, tuleb eristada, et millal võib teabe edastada privaatsuspoliitikas ja milline teave peab olema nõusoleku vormi juures.

3.3.2.3. Läbipaistvuse põhimõte teabe edastamisel

Teabe edastamisel on suur roll läbipaistvusel. Läbipaistvust pole andmekaitse määruses defineeritud, küll aga viitab määrus läbipaistvusele artikli 5 lõike 1 punktis a, mille kohaselt isikuandmete töötlemisel tuleb tagada, et töötlemine on andmesubjektile läbipaistev.[232] Andmekaitse määruse preambula punkt 39 annab läbipaistvuse kohta järgmised suunised:

"Läbipaistvuse põhimõte eeldab, et nende isikuandmete töötlemisega seotud teave ja sõnumid on lihtsalt kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud. Kõnealune põhimõte puudutab eelkõige andmesubjektide teavitamist vastutava töötleja identiteedist ning töötlemise eesmärgist ja täiendavast teabest, et tagada asjaomaste füüsiliste isikute suhtes õiglane ja läbipaistev töötlemine ning nende õigus saada neid puudutavate isikuandmete töötlemise kohta kinnitust ja sõnumeid." Oluline on ka, et teave oleks korrektne ja terviklik.[233] Teabe arusaadavust, selgust ja lihtsust on käsitletud peatükis 3.3.2.1.

Läbipaistvuse põhimõtte kohaselt tuleks vajaduse korral täiendavalt kasutada visualiseerimist.[234] Visualiseerimine tähendab, et andmesubjektile seletatakse näiteks liikuva pildi abil lahti, mille jaoks tema andmeid kasutatakse.

Andmesubjektile suunatud teabe võib esitada elektrooniliselt näiteks veebisaidi kaudu. Eriti asjakohane on see muudes olukordades, mille puhul osapoolte arvukuse ja kasutatava

[231] Näiteks Tele2 privaatsuspoliitika. Kättesaadav: https://tele2.ee/abi/lepingud-ja-arveldus/tingimused/iseteenindusportaali-minu-tele2-kasutustingimused-ja-privaatsuspoliitika. SEB Isikuandmete töötlemise üldpõhimõtted. Kättesaadav: https://www.seb.ee/tingimused/isikuandmete-tootlemise-uldpohimotted.
[232] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 141.
[233] *Ibid*, p 142.
[234] Andmekaitse määruse preambula punkt 58.

tehnoloogia keerukuse tõttu on andmesubjektil raske teada saada ja mõista, kas kogutakse tema isikuandmeid, kes neid kogub ja millisel eesmärgil, nagu näiteks veebireklaami puhul.[235]

Seega võib praktikas läbipaistvuse nõuete täitmiseks kliendile veebileheküljel kuvada ülevaate lihtsal ja arusaadaval viisil veebileheküljel privaatsuse alalehekülje all, mis andmeid kliendi kohta kogutakse, milleks neid kasutatakse ja mis on töötlemise õiguslik alus. Lisaks peaks seal olema välja toodud, kuidas klient saab oma valikuid hallata.

Samas võiks autori arvates informatsiooni esitamisel lähtuda ka mõistlikkuse põhimõttest. Kui ettevõte palub kliendil sisestada pakkumiste saatmiseks oma nime ja e-posti aadressi, on selge, et töödeldakse just neid andmeid ning eraldi sõnaselgelt ei pea välja tooma, milliseid andmeid töödeldakse.

Läbipaistvuse kohta käivad suunised on antud eraldi ka andmekaitse töörühm läbipaistvuse juhises. Selles on lisaks eelnevale rõhutatud, et läbipaistvuse nõude täitmiseks peab info olema andmesubjektile kättesaadav tasuta.[236] Vastasel korral takistaks finantsilised võimalused või näiteks tasu nõudmine informatsiooni saamist.

Üheks kohustuseks andmesubjekti informeerimisel on ka kohustus välja tuua andmekaitseametniku kontaktandmed (andmekaitse määruse art 13 lõige 1 b). Teisalt on töörühm seisukohal, et kui privaatsuspoliitikas on jäetud välja toomata, kuidas töötleja andmekaitseametnikuga saab ühendust võtta, on privaatsuspoliitika alusel kogutud nõusolekud siiski piisavalt informeeritud ning kehtivad.[237] Seega nõuete täitmata jätmine ei too igal juhul kaasa nõusoleku kehtetust. Samas kui kohustuse täitmata jätmine toob kaasa andmesubjekti isikuandmete sellise töötlemise, millega rikutakse andmekaitse määrust, on andmesubjektil siiski õigus kasutada andmekaitse määruses sätestatud tõhusat õiguskaitsevahendit (andmekaitse määruse art 79 lõige 1).

Andmekaitse määruse preambula punkti 61 kohaselt tuleb andmesubjekti isikuandmete töötlemist käsitlev teave anda talle juhtumi asjaoludest olenevalt kas andmesubjektilt andmete kogumise ajal või mõistliku ajavahemiku jooksul, juhul kui andmeid hangitakse muust allikast.

Seni pole Eestis isikuandmete töötlemise regulatsioon läbipaistvuse põhimõtet käsitlenud. Samas võib läbipaistvuse põhimõte haakuda teiste andmekaitse määrusest tulenevate põhimõtetega. Näiteks individuaalse osaluse põhimõttega, mille üheks osaks on isikuandmete

[235] Andmekaitse määruse preambula punkt 58.
[236] Article 29 Data Protection Working Party. Guidelines on Transparency Under Regulation 2016/679, p 9.
[237] *Ibid*, p 15.

töötlejale pandud kohustus teavitada andmesubjekti tema kohta kogutavatest andmetest (IKS § 6 p 7). Seega on Eesti õiguses läbipaistvuse põhimõte uueks kriteeriumiks ning ettevõtted peavad teabe esitamisel seda põhimõtet arvesse võtma. Küll aga on autor seisukohal, et läbipaistvuse põhimõte mõnevõrra kattub üldiselt teabe kättesaadavusel seatud nõuetega, mistõttu ei too see põhimõte kaasa olulist muudatust, kui teabe edastamisel võetakse arvesse juba kõiki eelnevalt käsitletud kriteeriume.

3.4. Ühemõttelisus

Vastavalt andmekaitse määruse artikli 4 punktile 11 peab nõusolek olema ühemõtteline. Ühemõtteline nõusolek peab olema antud selge tahteavaldust väljendava tegevusega. See tähendab, et eelnevalt märgistatud lahtreid, vaikimist ja tegevusetust ei peeta nõusolekuks (preambula punkt 32).

Ühemõttelisus tähendab, et ei tohiks olla põhjendatud kahtlust seoses sellega, et andmesubjekt tahtis väljendada nõustumist oma isikuandmete töötlemisega. Ühemõttelisuse käsitlemisel tuleb analüüsida nõusoleku andmise meetodeid ja hinnata, kas nendest järeldub üheselt mõistetav nõusolek. Selleks, et nõusolek oleks kehtiv ja andmekaitse määrusega kooskõlas, peab see väljenduma andmesubjekti ühemõttelises tahteavalduses. Kuna nõusolek võib olla väljendatud ükskõik millises vormis, peab olema selge, mis täpselt tahteavalduse alla kuulub. Minimaalne väljendus võiks olla andmesubjekti poolt mis tahes liiki signaal, mis on piisavalt selge, et olla võimeline andma edasi andmesubjekti soove ning olema töötleja poolt vastuvõetav.[238] Ühemõttelise nõusolekuga on tegemist näiteks "jah" sõna andmisega selgele nõusoleku taotlusele.[239]

Ühemõttelist nõusolekut ei saa eeldada vaid sellest, kui andmesubjekt kuidagi taotlusele ei reageeri, kuna tahteavalduse andmiseks on vajalik selge tegevus. Seega ei saa nõusolekut järeldada tegevusetuse tõttu. [240] Näiteks puudub nõusolek sõltumata andmesubjekti reaktsioonist olukorras, kus isikuandmete töötleja saadab andmesubjektile kirja, kus teavitab teda andmete töötlusest juhul, kui kirja saaja sellest kirjale vastamisega kümne päeva jooksul ei keeldu. Kuna andmesubjektidelt vaikimisega saadud nõusolek ei ole kooskõlas andmekaitse määrusega, ei saa lugeda kirjale õigeaegselt mitte vastanuid andmete töötlemisega nõustunuks.[241]

[238] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 11.
[239] Information Commissioner's office. Consultation: GDPR consent guidance, p 39.
[240] Fundamental Rights Agency, p 55.
[241] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 12.

Samamoodi ei ole määruse nõuetega kooskõlas nn *opt-out* põhimõttele tuginev nõustumust kinnitav märge, mis tehtud eelnevalt teksti juurde.[242] Eelmärgistatud kaste ei peeta piisavaks seetõttu, andmesubjekti kavatsus nõusoleku andmiseks ei tohi jääda mitmeti mõistetavaks. Kuna antud juhul käsitletaks nõusoleku andmisena tegevusetust ehk linnukese mitte-eemaldamist, siis ei saa sellisel viisil ühemõttelist nõusolekut anda.[243] Õige käitumisviis antud juhul oleks see, et vaikimisi oleks linnukese märkimise kastike tühi ning vajadusel andmesubjekt ise märgib linnukese kastikesse .

Ühemõttelisuse nõue kohustab andmetöötlejaid looma kindlaid protseduure üksikisikute nõusoleku andmiseks. Nimelt tuleb kas taotleda selgesõnaline nõusolek või kasutada teatud meetmeid, mis edastaksid üksikisikute selgesõnalise nõusoleku. Tahteavaldus peaks sisaldama soovi, milles andmesubjekt väljendab oma nõusolekut: see võib tähendada paberkandjal käsitsi antud allkirja, kuid ka suulisi avaldusi kokkuleppe sõlmimiseks või käitumist, millest tulenevalt saab järeldada, et nõusolek on antud. Näiteks kasti linnukese tegemine või infoühiskonna teenuste tehniliste sätete valimine on viisid, mis sobivad ühemõtteliselt nõusoleku andmiseks.[244]

Ühemõttelise nõusoleku saab anda ka anda lepingu sõlmimisel, kui lepingu blanketil on lahter, milles palutakse reklaamposti saamiseks lisada oma e-posti aadress. Kui isik, pärast e-posti aadressi esitamist reklaamposti lahtris lepingu allkirjastab, on tegemist ühemõttelise nõusolekuga. Sellisel juhul on nõusolek saadud nii selgelt kui ka kirjalikult.[245]

Eeltoodud näite puhul tuleb oluliseks piiritlemiskriteeriumiks pidada asjaolu, et andmesubjekti tegevus e-posti aadressi kirjutamisel ei saanud olla suunatud muule, kui nõusoleku andmisele. Samal ajal annavad eelnevad näited ettevõtjale ka tõendi nõusoleku olemasolust, kui ta seda hiljem säilitab.

Tegevusega nõusoleku andmisena saab käsitleda ka visiitkaardi jätmist lauale, kui eelnevalt on isikule selgitatud, et pakkumiste saatmiseks on ettevõttel vaja tema e-posti aadressi. Sama kehtib ka juhul, kui isik saadab ettevõttele oma nime ning aadressi eesmärgiga saada sealt informatsiooni. Viimase näite puhul tuleks tema tegevust mõista kui õigusliku aluse andmist isikuandmete töötlemiseks ulatuses, mis on vajalik tema taotluse töötlemiseks ja sellele

[242] A. Bussche, P. Voigt. The EU General Data Protection Regulation, 95.
[243] Information Commissioner's office. Consultation: GDPR consent guidance, p 23.
[244] *Ibid*.
[245] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 21.

vastamiseks.[246] Teisalt ei ole see piisav selleks, et asuda isikule saatma muud turunduslikku teavet.

Esineb ka olukordi, kus pole vaja selgesõnaliselt isikul öelda "jah, nõustun tingimustega", vaid ühemõttelist nõusolekut saab järeldada ka isiku käitumisest. Näiteks hotelli registreerimise ajal teavitab külaliste vastuvõtja, et pärastlõunal toimub pildistamine ühes hotelli kohvikutest hotelli turundusmaterjalide jaoks. Kliente teavitatakse, et kes soovib pildistamisel osaleda, võib kohvikut sel ajal külastada. Kes osaleda ei soovi, palutakse külastada teist kohvikut. Hotelli külastajad, kes on pildistamisest informeerituna otsustanud minna kohvikut külastama pildistamise ajal, võib käsitleda nende nõusolekuna nende pildistamiseks. Nõusolek tuleneb sellest, et hotelli külastajad lähevad kohvikusse, kus fotode tegemine samal ajahetkel toimub. Kohvikusse sisenemine kujutab endast isiku soovi pildistamiseks.[247] Teisalt tekib ka siinkohal tõsine tõenduslik probleem, kuivõrd on vähetõenäoline, et klientide suulist informeerimist suudetakse tõendada.

Eeltoodust järeldub, et nõusoleku ühemõttelisuse nõude tõttu on andmetöötlejad sunnitud kasutama meetodeid, mis tagaks hilisema tõendamisvõimaluse nõusoleku olemasolu kohta.

Isikuandmete töötleja ei saa küsida nõusolekut sama tegevuse läbi, kui näiteks nõustumine lepinguga või nõustumine teenuse tingimustega, kuna kõikehaaravat tingimuste aktsepteerimist ei saa lugeda selgeks kinnitavaks tegevuseks.[248] See tuleneb eelnevalt käsitletud põhimõttest, mille kohaselt nõusolek peab olema ka selge ja eristatav muudest küsimustest (andmekaitse määruse art 7 lg 2).

Ka ekraanil viipamine, lehvitamine nutikate kaamerate ees või nutitelefoni teatud viisil liigutamine võivad viidata lepingu sõlmimisele tingimusel, et eelnevalt on esitatud on selgitus ja on selge, et kõnealune ettepanek tähistab konkreetsele lepingule nõusoleku andmist. Selliseks selgituseks võib olla enne nõusoleku andmist eelnenud teave, et lohistades riba vasakule, nõustute isikuandmete töötlemisega kirjeldatud eesmärgil.[249]

Teisalt ei saa andmesubjekti nõusolekut järeldada vaid sellest, et ta on tingimused läbi lehitsenud, kui tingimuste läbi lehitsemisel loetakse nõusolek antuks.[250] Selle põhjuseks on asjaolu, et andmesubjekt ei pruugi hoiatusteadet märgata, kui ta lehitseb teksti edasi liiga kiiresti. Seega pole antud selgitus piisavalt selge, kui tavapärase hoolsuse korral võib see

[246] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 11.
[247] *Ibid*, p 23.
[248] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 16-17.
[249] *Ibid,* p 17.
[250] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 23.

andmesubjektile jääda ekslikult tähelepanuta. Seega tuleb eriti hoolikas olla ühemõttelisuse nõude järgimisel juhtudel, kui tingimusi on võimalik aktsepteerida ilma neid läbi lehitsemata.

Nõusoleku ühemõttelisuse hindamise muudab keeruliseks asjaolu, et mitte kõik nõusoleku vormid, mis võivad esmapilgul tunduda selgesõnalised, ei ole tegelikult nõusolekuks piisavad. Nii on Euroopa Kohus kohtuasjas *Volker und Markus Schecke* vs. *Land Hessen* käsitlenud ELi fondide kasusaajate nimede ja kasu suuruse avaldamist. Kohtujurist analüüsis, kas üheselt mõistetava nõusoleku tingimused olid täidetud juhul, kui isikud olid allkirjastanud avalduse, milles öeldi: "Olen teadlik, et määruse [...] nr 1290/2005 artikkel 44a nõuab, et avaldatakse teavet [rahaliste vahendite] kohta EAGF ja EAFRD ning iga toetusesaaja kohta saadud summad."[251]

Kohtujurist leidis, et üksnes teatavaks võtmine, et mingisugune isikuandmete avaldamine võib toimuda, ei ole sama, mis ühemõttelise nõusoleku andmine. Samuti ei ole tegemist vabalt antud konkreetse tahteavaldusega artikli 2 punkti h mõistes. Seetõttu järeldas kohtujurist, et hagejad ei ole andnud oma nõusolekut nende isikuandmete töötlemiseks (st avaldamiseks) direktiivi 95/46/EÜ artikli 7 punkti a tähenduses.[252] Töö autor nõustub kohtujuristi seisukohaga, kuna isiku avaldusest ei tohi jääda kahtlust, kas nõusolek on antud või mitte.

Ühemõttelisuse nõue ei keela suulise nõusoleku andmist. Näiteks hotellist välja registreerides küsib klienditeenindaja klientidelt, kas nad sooviksid oma aadressi esitada, et hotell saaks neile reklaamsõnumeid saata. Isikud, kes pärast teenindaja ettepaneku ära kuulamist ja asjakohase teabe saamist vastavad oma postiaadressi andmisega, annavad otsese selge nõusoleku, kuna andmesubjekti tegevust saab mõista ühemõttelise avaldusena.[253] Siiski tekib töötleja jaoks probleeme tõendamisel. Kui andmetöötleja suudab ära näidata, et ta hotelli broneeringu tegemiseks ei küsi isikutelt kodust aadressi, siis on tõenäoline, et isik pidi andma selle muul põhjusel. Kui aga juba broneeringu tegemisel küsib hotell isikult nõusolekut, siis on keeruline vaid suulisele nõusolekule tuginedes tõendada, et isik on andnud oma koduse aadressi ka pakkumiste edastamiseks. Ühemõttelisusega seondub ka probleem andmetöötleja tuvastamatusega. Enne nõusoleku küsimist peab andmetöötleja olema piisavalt kindel, et nõusolekut andev isik on tegelikult andmesubjekt. See on eriti oluline siis, kui nõusolek antakse

[251] Opinion of Advocate General Sharpston delivered on 17 June 2010, *Volker und Markus Schecke GbR*, in Joined Cases C-92/09 and C-93/09.
[252] Opinion of Advocate General Sharpston delivered on 17 June 2010, *Volker und Markus Schecke GbR*, in Joined Cases C-92/09 and C-93/09. It should be noted that the ECJ ruled in its judgment of 9 November 2010 that the data processing was not based on consent: "63. The European Union legislation in question, which merely provides that beneficiaries of aid are to be informed in advance that the data concerning them will be published, thus does not seek to base the personal data processing for which it provides on the consent of the beneficiaries concerned.
[253] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 22.

telefoni või interneti vahendusel.[254] Kui nõusolekut pole andnud andmesubjekt, pole nõusolek kehtiv. Eriti oluline on tuvastada õige isik lapse isikuandmete töötlemisel.

Sarnaselt andmekaitse määruses sätestatule ei loeta IKS-is vaikimist või tegevusetust nõusolekuks (IKS § 12 lg 1 ls 3). Ühemõttelise nõusoleku põhimõtete tuvastamiseks Eestis kehtiva õiguse alusel tuleb vaadata täiendavalt veel tsiviilseadustiku üldosa seaduse tahteavalduse andmise põhimõtteid. Peatükis 2.2 on selgitatud, et tahteavaldus võib olla nii otsene kui ka kaudne. Otseses tahteavalduses väljendub tahe tuua kaasa õiguslik tagajärg sõnaselgelt, kas suulises või kirjalikus avalduses.[255] Ka kaudse tahteavaldusega saab väljendada ühemõttelist nõusolekut, kui selles väljendub tegu, millest saab järeldada tahet tuua kaasa õiguslik tagajärg.[256] Samas lubab kehtiv IKS suulist nõusolekut anda väga erandlikel juhtudel. Seega peab selge tahteavaldus väljenduma eelkõige siiski kirjalikku taasesitamist võimaldavas vormis.

2018. a. IKS-i eelnõu ühemõttelisust ei käsitle. Järelikult annab andmekaitse määrus justkui vabastuse seni kehtinud vorminõudest, kuna Eesti õigus ei võimaldanud nõusolekut anda suuliselt, välja arvatud juhul, kui vorminõude järgmine ei ole andmetöötluse erilise viisi tõttu võimalik (IKS § 12 lg 2). Autori hinnangul annab andmekaitse määrus sellega ettevõtetele nõusoleku küsimiseks paindlikkust juurde, kuid eeldusel, et ettevõte suudab suulise nõusoleku andmist tõendada.

3.5. Selgesõnalisus

Andmekaitse määrusest tuleneb lisaks eelmises peatükis sätestatud nõusoleku tingimustele teatud juhtudel täiendavalt sõnaselge nõusoleku esitamise nõue. Andmekaitse määruse alusel peab nõusolek olema sõnaselge isikuandmete eriliikide töötlemisel (artikkel 8 lõige 2 punkt a), andmete edastamisel kolmandatesse riikidesse või rahvusvahelistele organisatsioonidele, kui puuduvad piisavad tagatised (artikkel 49) ja automatiseeritud otsusete, sealhulgas profileerimise puhul (artikkel 22).

Andmekaitse määrus ei selgita, mida selgesõnaline nõusolek tähendab. Lisaks on seda keeruline eristada ühemõttelisest nõusolekust. Õiguskirjanduses on asutud seisukohale, et selgesõnaline nõusolek (ing. k *explicit consent*) artikli 8 mõistes ja otsene tahteavaldus (ing. k *express consent),* mis on oluline ühemõttelise nõusoleku juures, omavad juriidiliselt sama tähendust. See hõlmab kõiki olukordi, kus üksikisikutele esitatakse ettepanek nõustuda või mitte nõustuda

[254] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 21.
[255] P. Varul. TsÜS komm, lk 221.
[256] *Ibid*, lk 222.

nende isikuandmete konkreetse kasutamise või avalikustamisega ning nad vastavad nõusoleku päringule aktiivse tegevusega suuliselt või kirjalikult.[257] Vahe tegemine selgesõnalisuse ja ühemõttelisuse vahel on keeruline ka seetõttu, et ka andmekaitse määruse artiklis 7 toodud nõusoleku nõudeid kohaldatakse ka selgesõnalise nõusoleku andmisel.[258]

Põhiline erinevus nõusoleku selgesõnalisuse ja ühemõttelisuse vahel seisneb õiguskirjanduses toodu kohaselt selles, et selgesõnaline nõusolek tuleb ka selgesõnaliselt (suuliselt või kirjalikult) kinnitada. Nõusoleku definitsioonist tuleneb, et nõusoleku saab anda kas avalduse vormis või selge nõusolekut väljendava tegevusega. Selgesõnalise nõusoleku andmiseks sobib aga üksnes avalduse vorm.[259] Nõusolekut väljendav tegevus, nii nagu ühemõttelise nõusoleku juures, ei ole seega selgesõnaline nõusolek, mida saaks näiteks eriliigiliste isikuandmete töötlemiseks kasutada. Seega on siin erinevus nõusoleku ühemõttelisuse kriteeriumiga, kuna ühemõttelist nõusolekut saab tegevusega anda juhtudel, mis ei vaja selgesõnalist nõusolekut.

Seega tähendab selgesõnalisus, et nõusoleku nõuded pole täidetud nõustumust kinnitava teksti juurde märke tegemisega selleks ette nähtud kasti või e-posti aadressi sisestamisega vajalikku lünka. Seeläbi muutub ettevõtete jaoks veel keerulisemaks isikuandmete töötlemine olukordades, kus nõutakse selgesõnalist nõusolekut. Üheks võimaluseks on ettevõttel mõelda välja lause, milles oleks selgesõnalisuse nõue täidetud ning paluda see juhul, kui klient töötlemisega nõustub, selgesõnalisuse kindlustamiseks ka omakäeliselt välja kirjutada. Kindluse tagab veel enamgi, kui eelnevalt toodud olukorras kirjalik avaldus ka andmesubjekti poolt allkirjastatakse. [260] Samas võiks autori hinnangul selgesõnalisuse nõue olla täidetud ka juhul, kui andmetöötleja annab ise nõusoleku sisu ette ning kliendi ülesandeks jääb see üksnes allkirjastada.

Internetis saab selgesõnalist nõusolekut anda elektroonilist vormi täites, mille lõpus antakse selgesõnaline nõusolek digitaalallkirja abil. Samas ei tähenda see, et selgesõnalist nõusolekut saab anda üksnes kirjalikus vormis või allkirjaga.[261]

Selgesõnalise nõusolekuga on tegemist ka kahe-etapilise kinnituse (ingl. k. *double opt-in*) juures.[262] Kahe-etapiline kinnitus on nõusoleku andmise viis, millega andmesubjekt esmalt annab nõusoleku ning hiljem kinnitab selle üle. Näiteks kui klient annab andmete töötlemiseks nõusoleku sisestades enda e-posti aadressi, saadab töötleja andmesubjektile kinnituseks e-kirja

[257] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 25.
[258] Information Commissioner's office. Consultation: GDPR consent guidance, p 24.
[259] *Ibid*, p 24.
[260] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 18.
[261] *Ibid*.
[262] *Ibid,* p 19:

või SMS-i, mis sisaldab linki. Ainult siis, kui klient lingi avab ning oma andmed kinnitab, on kahe-etapiline nõusolek antud.[263] Kahe-etapiline kinnitus on eriti oluline just nõusoleku küsimisel internetis, kuna andmekaitse määrus ei sätesta selle saamise jaoks formaalseid nõudeid. Sellisel viisil saab ettevõte olla kindel, et keegi ei väärkasuta andmesubjekti e-posti aadressi ehk ei esine kellegi kolmandana.[264]

Samas kui andmekaitse määruse tõlgenduste kohaselt tuleb ettevõtetel hakata nõusolekuid küsima kahe-etapiliselt, suurendab see ettevõtete halduskoormust, kuna see tähendab põhjalikumat süsteemi üles ehitust. Lisaks loob kahe-etapiline süsteem täiendava kontrollikohustuse. Teisalt on see süsteem vajalik selleks, et ettevõtted saaks siiski nõusoleku olemasolus kindlad olla. See aga näitab, kui põhjalike meetmeid ettevõtted peavad ette võtma, et saada internetis andmesubjektilt selgesõnaline nõusolek.

Töö autori hinnangul on sellise eraldi instituudi kehtestamine põhjendamatu, kui selle ainuke sisulise vajadus ja toime on nõusolekule justkui vorminõude kehtestamine, kuna eelnevast saab järeldada, et selgesõnalise nõusoleku jaoks on vaja kirjaliku tahteavaldust juhul. Kui nõusolek võetakse kahe-etapilise kinnitusena, siis tuleb kinnitus anda vähemalt kirjalikku taasesitamist võimaldavas vormis. Kuna käesoleval juhul on vorminõue peidetud vormireeglile mitte viitava kriteeriumi taha, võib selgesõnalisuse nõude selline kohaldamine olla ettevõtetele segadust tekitav.

Eesti kehtivas regulatsioonis ei näe IKS ette selgesõnalise nõusoleku nõuet määruses toodud juhtumite töötlemisel. Automatiseeritud otsuste tegemise kohta näiteks puudub IKS-is viide sellele, et seda võiks teha nõusoleku alusel (IKS §-d 17 ja 18). Kolmandatesse riikidesse edastamine on lubatud IKS § 18 lõike 5 punkti 1 alusel, kuid seejuures ei nähta nõusolekule ette täiendavaid nõudeid. Täiendav nõue on ette nähtud üksnes delikaatsete isikuandmete töötlemiseks, mille kohaselt tuleb andmesubjektilt tuleb saada nõusolek kirjalikku taasesitamist võimaldavas vormis (IKS § 12 lg 4). Kui nõusolek tuleb võtta uue regulatsiooni kohaselt kirjalikult või kahe-etapilise kinnitusena, on tegemist uue nõudega, mida tuleb ettevõtetel kohaldama hakata. Selgesõnalisuse nõude praktiline tähendus jääb aga ilmselt piiratuks, kujutades endast vaid peidetud täiendavat vorminõuet kehtivale nõusolekule.

2018. a. IKS-i eelnõu ei selgita selgesõnalisuse nõudeid, mistõttu tuleb lähtuda andmekaitse määruse alusel tõlgendatud seisukohast.

[263] A. Bussche; P. Voigt. Data protection in Germany: including EU General Data Protection Regulation. Berlin: Springer 2018, p 40.
[264] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 93.

3.6. Tagasivõetavus

Andmekaitse määruse artikkel 7 lõige 3 sätestab, et vastutav töötleja peab tagama andmesubjektile õiguse võtta igal ajal nõusolek tagasi ning seda sama lihtsalt kui nõusoleku andmisel. Seejuures on töötlejal kohustus andmesubjekti enne nõusoleku andmist sellest õigusest teavitada. Tagasivõetavus on muuhulgas üks vabatahtlikkuse olulisi elemente.[265]

Kui lõppkasutajad on andnud oma nõusoleku otseturunduslike mittetellitud teadaannete saamiseks, siis peaks neile alati jääma võimalus oma nõusolekust lihtsasti loobuda (e-privaatsuse määruse preambula p 34). Lihtne loobumine tähendab, et e-posti teel otseturundusteadaandeid saatvad juriidilised isikud peavad teadaandele lisama lingi või kehtiva elektronposti aadressi, mida lõppkasutajad saavad kasutada oma nõusoleku tagasivõtmiseks. Häälkõnede ja automatiseeritud numbrivalimis- ja sidesüsteemide abil otseturundusteadaandeid edastavad juriidilised isikud peaksid kuvama liini numbri, millele saab ettevõttele helistada, või lisama oma numbrile konkreetse koodi, mis näitab, et tegemist on turundusliku kõnega (e-privaatsuse määruse preambula p 35). Kui turundusteadaanne saadetakse SMS-i teel, peaks SMS sisaldama infot, kuidas pakkumisest loobuda. Näiteks võiks olla SMS-i lõpus viide numbrile, millele sõnumit saates tellimus tühistatakse.

Eelnev tähendab, et tagasivõtmise õiguse peab sõnaselgelt välja tooma enne nõusoleku andmist, kuid siis kui nõusolek on antud, ei pea seda õigust igakordselt reklaamipostituse saatmisel välja tooma, vaid piisab üksnes viitamisest kohale, kus saab pakkumistest loobuda.

Nõusoleku tagasivõtmine ei tohi olla andmesubjekti jaoks koormavam või keerulisem kui oli selle andmine. Näiteks müüb muusikafestival pileteid internetis tegutseva vahendaja kaudu. Iga veebipileti müügiga küsitakse nõusolekut, et kasutada kontaktandmeid turunduslikel eesmärkidel. Sel eesmärgil nõusoleku andmiseks saavad kliendid valida kas “ei” või “jah”. Kui andmesubjekt saab anda nõusoleku tema kontaktandmete turunduslikel eesmärkidel kasutamiseks veebileheküljel „jah“ või „ei“ valimisega, kuid loobumiseks peavad nad telefoni teel pöörduma kõnekeskuse poole, mida saab teha üksnes tööpäeviti kell 8.00-17.00,, siis pole nõusoleku tagasivõtmine andmekaitse määrusega kooskõlas. nõusoleku tühistamine üksnes läbi tööajal telefonikõne tegemise on koormavam kui oli nõusoleku andmine ühe hiireklõpsuga, mida saab teha tööpäeva ringselt.[266]

[265] A. Bussche, P. Voigt. The EU General Data Protection Regulation, p 95.
[266] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 21.

Seega kui nõusolek saadakse elektroonilisel teel ainult ühe hiireklõpsu, viipamise või klahvikombinatsiooni abil, peavad andmesubjektid saama praktikas seda nõusolekut võrdselt sama hõlpsasti tagasi võtta ehk vähemalt sama lihtsate meetmete läbi.

Nõusoleku tagasivõtmisel ei tohiks olla muid negatiivseid tagajärgi peale selle, et andmesubjekt ei saa enam isikuandmete töötlemise tulemusena pakutud hüve. Samuti ei tohiks kohustada andmesubjekti loobumist põhjendama. Kui klient nõustus oma andmete kasutamisega reklaamposti saamiseks ning sai vastutasuks ettevõtte poolt 5% allahindlust, ei pea nõusoleku tagasivõtmisel isik allahindluse summat tagasi maksma, kuna sellisel juhul oleks tegemist negatiivse tagajärjega.[267] Seega kui isikule saabuks nõusoleku tagasivõtmisel kohustus näiteks tasu maksmise näol, võib saabuda oht, et andmesubjektid ei võtaks nõusolekuid tagasi.

Nõusoleku tagasivõtmisel on kõik töötlustoimingud seaduslikud, mis on tehtud kuni tagasivõtmise hetkeni, kuid vastutav töötleja peab pärast nõusoleku tagasivõtmist töötlemistoimingud lõpetama. Kui andmete töötlemise (nt täiendav säilitamine) õigustamiseks ei ole muud seaduslikku alust, tuleks töötlejal need kustutada või anonüümseks teha.

Olukorras, kus 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 õiguslikule alusele. Lisaks tuleb igast õigusliku aluse muutumisest teavitada andmesubjekti vastavalt artiklites 13 ja 14 sätestatud teabele esitatavatele nõuetele ja läbipaistvuse üldpõhimõtetele.[268] Teisalt on leitud, et kui juba töötlemise käigus ilmus uus õiguslik alus ning seda alust saab õiguspäraselt kohaldada, siis võib töötlemine jätkuda.[269]

Autori hinnangul tuleb eelneva puhul eristada kahte olukorda. Nõusoleku tagasivõtmisel ei saa minna üle uuele õiguslikule alusele siis, kui seda on vaja üksnes töötlemise õigustamiseks, kuna ettevõte ei taha näiteks loobuda isikule pakkumiste saatmisest. Teine olukord on seotud juhtumiga, kus ettevõte võib olla isikuandmete töötlemise seaduslikkuse tagamiseks ekslikult tuginenud nõusoleku vajadusele aga hiljem selgub, et töötlemise õige alus on hoopis leping. Sellisel juhul saab ettevõte ikkagi tugineda sellele, et isikuandmete töötlemine on lepingu täitmiseks vajalik (andmekaitse määruse art 6 lg 1 p b), kuna vastasel juhul tooks nõusoleku tagasivõtmine olukorra, kus lepingut poleks enam võimalik täita. Tegemist on autori arvates mõistliku lahendusega, kuna on tõenäoline, et ettevõtted võivad õigusliku aluse valimisel

[267] Fundamental Rights Agency, p 58.
[268] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 22.
[269] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 13.

eksida. Kui on tuvastatud õige õiguslik alus ning selle kehtivuse eeldused on täidetud, siis võib töötlemine jätkuda hoopis teisel õiguslikul alusel. Seega ei saa tekkida olukord, kus ettevõte võiks teadlikult valida vale õigusliku aluse, kuna isikuandmete töötlemise kehtivuseks peaks ettevõttel olema täidetud ühe õigusliku aluse kehtivuse eelduste asemel kahe õigusliku aluse eeldused.

Kui klient võtab nõusoleku tagasi, tekib küsimus, kui kiirelt peab töötlemine lõppema. Õiguspraktikud leiavad, et töötlemise peab lõpetama koheselt, eriti automatiseeritud keskkonnas internetis. Samas nenditakse, et mõningal juhul siiski on õigustatud mõningane hilinemine. [270] Samas pole täpsustatud, millisel juhul on hilinemine õigustatud. Autori hinnangul võiks see kõne alla tulla juhul, kui ettevõttel pole nõusoleku tagasivõtmiseks ressurssi arendada automaatne süsteem, vaid tagasivõtmine vajab inimtegevust.

Õigus nõusolek tagasi võtta teeb nõusolekule tuginemisele seega ettevõtetele keerulisemaks, kuna nad peavad olema nõusoleku tagasivõtmiseks koheselt valmis.

Sarnaselt andmekaitse määrusega lubab ka praegu kehtiv IKS § 12 lõike 7 alusel andmesubjektil nõusolekut igal ajal tagasi võtta. Nõusoleku tagasivõtmisel ei ole IKS § 12 lõike 7 alusel tagasiulatuvat jõudu ning nõusoleku suhtes kohaldatakse täiendavalt tsiviilseadustiku üldosa seaduses tahteavalduse kohta sätestatut.

Lisaks õigusele igal ajal nõusolek tagasi võtta nägi IKS ette juba nõusoleku andmisel õiguse keelata oma andmete töötlemine, kuid seda üksnes tarbijaharjumuste uurimiseks või otseturustamise eesmärgil kas üldse või üksnes nende andmete üleandmine kolmandatele isikutele (või osale neist), kes sooviksid andmeid kasutada tarbijaharjumuste uurimiseks või otseturustamiseks. [271]

Tagasivõtmise õigus võib aga tekitada nõusoleku saajale palju ebamugavusi. Näiteks isik annab kehtiva õiguskorra alusel nõusoleku valmistada endast eluloofilm. Selleks on vaja töödelda suures mahus eluloofilmi subjekti isikuandmeid. Kehtiv õiguskord ei näe sellises olukorras ette erandit, mille puhul nõusolekut töötlemiseks pole vaja, seega peab töötlemine toimuma nõusoleku alusel. IKS § 12 lõike 7 kohaselt võib andmesubjekt nõusoleku igal ajal tagasi võtta. See tähendab, et nõusolek võidakse tagasi võtta ka alles õhtul enne eluloofilmi esilinastust ning andmesubjektile ei järgne IKS-i kohaselt mingit vastutust, kuna isikuandmete töötlemiseks nõusoleku andmisel on tegemist erandiga üldisest tsiviilõigusest, mille kohaselt nõusoleku tagasivõtmisel ei tohi andmesubjektile saabuda õiguslike tagajärgi. Selline juhtum põhjustab

[270] Information Commissioner's office. Consultation: GDPR consent guidance, p 37.
[271] Isikuandmete kaitse seaduse seletuskiri. 1026 SE, lk 14.

aga olukorra, kus filmitootjal puudub järsku õigus filmi esitada ning võib filmitootjale tuua kaasa kahju, kui ta ei saa filmi valmistamiseks tehtud kulutusi piletimüügi näol tagasi teenida.

Õiguskirjanduses on leitud, et võimalus ilma õiguslike tagajärgedeta tahteavaldus tagasi võtta, on vastuolus üldise õiguse põhimõtetega, kuna selline tahteavaldus ei too endaga õiguspärast ootust nõusoleku püsimajäämisele.[272]

Autori hinnangul oleks sellises olukorras tegemist andmesubjekti poolt pahatahtliku käitumisega, mistõttu võiks filmitegija tugineda VÕS §-ile 6, mille kohaselt pooled peavad käituma heas usus. VÕS § 6 lõike 2 kohaselt ei kohaldata pahauskliku käitumise korral seadust. Seega saab filmitegija pahausklikult nõusoleku tagasivõtmisel jätta kõrvale seadusest tuleneva kohustuse töödelda isikuandmeid üksnes nõusoleku alusel ning see annab talle võimaluse ikkagi film avalikustada.

Nõusoleku tagasivõtmine on andmekaitse määruse kohaselt üks andmesubjekti õigustest, mille puhul liikmesriigil täiendav otsustusvõimalus puudub (andmekaitse määruse art 7 lg 3). Nagu peatükis 2.7.3. kirjeldatud, on liikmesriikidele jäetud andmekaitse määruse artikliga 85 võimalus siiski otsustada nõusoleku vajaduse üle kirjanduse ja kunsti valdkonnas. Seda võimalust on ka Eesti 2018. a. IKS-i eelnõus soovitud kasutada. Seega 2018. a. IKS-i eelnõu § 10 aitaks kõnealust probleemi lahendada sellega, et enam poleks isikult nõusolekut vaja. See annab filmitegijale kindlustunde, et saab eluloofilmi avalikustada. Siiski on vabastuse piiriks see, kui töötlemine ei kahjusta ülemääraselt andmesubjekti õigusi (2018. a. IKS-i eelnõu § 10 lg 1).

Eelnevast saab järeldada, et kuigi 2018. a. IKS-i eelnõu ei reguleeri nõusoleku tagasivõetavust, lahendab see erandite kehtestamisega, mil nõusolekut pole vaja, mõningad seni kehtivas regulatsioonis olnud probleemid.

3.7. Nõusoleku vorm ja tõendamisküsimused

Andmekaitse määrus ei sea nõusolekule vorminõuded. Andmekaitse määruse artikkel 4 punkt 11 sätestab, et nõusolek antakse kas avalduse vormis või selge nõusolekut väljendava tegevusega, mida on täpsemalt lahti selgitatud nõusoleku ühemõttelisust käsitletavas peatükis 3.4.

Sarnaselt andmekaitse määrusele puudus vorminõue ka andmekaitse direktiivis, kuid Eesti seadusandja oli teatud vorminõude siiski IKS-is kehtestanud. Kehtiv isikuandmete kaitse

[272] M. Männiko, lk 54.

seadus näeb ette vähemalt kirjalikku taasesitamist võimaldavat vormi, välja arvatud juhul, kui vorminõude järgmine ei ole andmetöötluse erilise viisi tõttu võimalik (IKS § 12 lg 4 ls 1). Seda, millisel juhul võiks tegemist olla andmetöötluse erilise viisiga, pole kehtiv seadus täpsustanud. Seega ei nähtud tänases isikuandmete kaitse regulatsioonis kindlat vormi ette, vaid vorminõue sõltus andmetöötluse viisist.

Kuna andmekaitse määruses vorminõuet pole kehtestatud, tekib küsimus, kas vorminõude kaotamine lihtsustab Eestis nõusoleku küsimist.

Autor on seisukohal, et ehkki formaalselt võib vorminõude kaotamine nõusoleku küsimist lihtsustada, on praktilistel kaalutlustel ka tulevikus soovitatav küsida nõusolek vähemalt kirjalikku taasesitamist võimaldavas vormis. Nõusoleku alusel töötlemisel on ettevõttel kohustus tõendada, et nõusolek on tegelikult ka antud. Tõendamiseks ei piisa üksnes ettevõtte väitest, et klient andis suuliselt oma nõusoleku näiteks 2 kuud tagasi, vaid tõendamiseks peab maha jääma mingi jälg nõusoleku andmisest. Seega tuleks hoolimata vorminõude puudumisest, küsida nõusolek siiski nii, et vaidluse korral oleks ettevõttel midagi ette näidata. Kõige kindlam oleks küsida nõusolek kirjalikult, e-maili teel või veebikeskkonnas konkreetse lehekülje kaudu. Samuti on võimalik suulise nõusoleku puhul saata hiljem kinnituskiri, milles klient peab nõusoleku üle kinnitama vajutades lingile (nö kahe-etapiline kinnitus, mida lähemalt kirjeldatud peatükis 3.5.).

Selleks, et ettevõtetel oleks võimalik nõusoleku olemasolu tõendada, ei piisa ainult nõusoleku kirjalikus vormis saamisest, vaid ettevõtted peavad neid nõusolekuid ka säilitama. Seega peaks olema andmetöötleja huvides koguda nõusolek nii, et seda saaks ka säilitada. [273]

Kui nõusolek on võetud internetis, peab ettevõte ehitama üles süsteemi, mis nõusolekuid kindlasse kohta salvestab. Määrus ei näe ette, milline info on täpselt vaja säilitada. Üldiselt on leitud, et töötleja peab säilitama info nõusoleku küsimise päringust ning vastusest. [274] Teisalt peab salvestusest nähtuma ka see, kes, millal ja kuidas nõusoleku andis ning mis oli nõusoleku sisu.[275] Kõige lihtsam on säilitada üks ühele seda teksti, mis kliendile ette anti ning säilitada ka kliendi vastust, kui sealt välja loetav kogu vajalik info.

Paberkandjal nõusolekuid võttes peab ettevõte looma aga turvalise koha, kus neid nõusolekuid säilitatakse, et tagada andmete turvalisus. Andmekaitse määruse alusel peab vastutav töötleja rakendama asjakohaseid meetmeid, et tagada andmesubjekti õiguste kaitse (andmekaitse

[273] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 26.
[274] Lee A. Bygrace. Data Privacy Law. An International Perspctive, p 161.
[275] Information Commissioner's office. Consultation: GDPR consent guidance, p 3.

määruse art 25 lg 1). Seega peab ettevõte peab kontrollima, kas andmekaitse määruse alusel piisab üksnes taotluste kapis hoidmisest või peab kapp olema ka lukustatud, et sinna kolmandad isikud juurde ei pääseks. Ka 2018. a. IKS-i eelnõus nähakse vastutavale töötlejale ette kohustus kehtestada töödeldavate isikuandmete säilitamise tähtaeg (2018. a. IKS § 21 lg 1). Tähtaja lõppemisel on kohus aga isikuandmed jäädavalt kustutada (2018. a. IKS § 21 lg 3). Seega olukorras, kus seaduses säilitamise tähtaega ei ole kehtestatud, on jäetud vastutavale töötlejale ülesanne kehtestada isikuandmete säilitamise tähtaeg. Isikuandmeid ei ole lubatud säilitada vajalikust kauem, mistõttu tuleb isikuandmed kustutada pärast säilitamise tähtaja lõppemist jäädavalt.[276]

Nõusoleku säilitamise kohta on selgitatud, et nõusolekut tuleb tõendada niikaua kuni kõnealune andmetöötlustoiming kestab. Pärast töötlemise lõppu tuleks nõusolekut säilitada vastavalt andmekaitse määruse artikli 17 lõikele 3 punktidele b ja e toodud juriidiliste kohustuste täitmiseks või juriidiliste nõuete koostamiseks, esitamiseks või kaitsmiseks.[277]

Ettevõtetel oleks siiski vaja lähtuda mingisugusest ajalisest raamistikust, et luua automaatne süsteem, kus nõusolekuid säilitatakse. Ajalise raamistiku paika panemisel saab lähtuda tsiviilseadustiku üldosa seaduses sätestatud nõude aegumise sätetest. Kuna nõusoleku nõue tuleneb seadusest, siis saab andmesubjekt tsiviilseadustiku üldosa seaduse § 149 alusel nõude esitada 10 aasta jooksul alates nõude sissenõutavaks muutumisest.Tõendamise küsimuse juures on oluline vastutaval töötlejal ära näidata ka seda, et andmesubjekti teavitati vajalikust informatsioonist, mis on välja toodud peatükis 3.3.[278] Nii teavitamiskohustuse kui ka muude nõusoleku tingimuste rikkumine võib kaasa tuua kuni 20 miljoni euro suuruse trahvi või 4% või ettevõtja puhul kuni 4 % tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem (andmekaitse määruse art 83 lg 5 p 1).

Kehtiv IKS § 12 lõige 8 selgitab, et nõusoleku olemasolu peab tõendama töötleja. Samast lõikest tuleneb põhimõte, mille kohaselt vaidluse korral eeldatakse, et isik ei ei ole oma isikuandmete töötlemiseks nõusolekut andnud. Seega on ka IKS-i kohaselt oluline nõusolekute kogumisel nende säilitamine, et vajadusel saaks nõusoleku olemasolu tõendada. Järelikult nõuete erinevus IKS-i ja andmekaiste määruse vahel pole nii oluline. Kuigi andmekaitse määrus annab võimaluse küsida nõusolek ka suuliselt, ei muutu siiski põhimõte, mille kohaselt ta peab

[276] Isikuandmete kaitse seaduse eelnõu seletuskiri. 06.11.2017, lk 26.
[277] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 20.
[278] *Ibid*.

suutma seda ka ära tõendada, mistõttu on suulise nõusoleku võtmiseks vajalik siiski täiendavaid reegleid rakendada.

Eelnevast saab järeldada, et kuna isikuandmete töötleja peab olema võimeline tõendama kehtiva nõusoleku andmist andmesubjekti poolt, ei oma vorminõude kaotamine sisulist mõju nõusoleku regulatsiooni lihtsustamisel.

2018. a. IKS-i eelnõu ei sea samuti nõusolekule vorminõuet, mistõttu ei peatu autor sellel pikemalt.

3.8. Nõusoleku kehtivus

3.8.1. Nõusoleku ajaline kehtivus

Andmekaitse määruses ei ole sätestatud konkreetset tähtaega nõusoleku kehtivuse kohta. Aja jooksul võib siiski tekkida kahtlus, kas nõusolek, mis on antud kehtivatel alustel, jääb ka tulevikus kehtima. Nimelt muudavad inimesed aja jooksul sageli oma varasemaid seisukohti, kuna nende esialgsed valikud olid hiljem nende arvates halvasti tehtud või muudetakse seisukohti mingite asjaolude muutumise tõttu.

Varasemalt on õiguskirjanduses leitud, et andmetöötlejad peaksid heade tavade tõttu püüdma mõne aja jooksul üksikisiku valikuid läbi vaadata, näiteks teavitama neid oma praegusest valikust ja pakkuma võimalusi oma senist valikut kas üle kinnitada või tühistada. Asjaomane periood sõltub loomulikult igast konkreetset juhtumist ja selle asjaolusid arvesse võttes.[279] Samas on peatükis 3.1.1. leitud, et valikute uuendamiseks peab siiski olema andmesubjekt olema turundusinfo saatmisega nõustunud. Sama põhimõtet saab ka kohaldada kõnealuse juhtumi puhul.

Nõusoleku kehtivus sõltub seega kontekstist, esialgse nõusoleku ulatusest ja andmesubjekti ootustest.[280] Kui töötlemistoimingud muutuvad või märkimisväärselt arenevad, siis esialgne nõusolek enam ei kehti. Lisaks võidakse nõusolekus sätestatud eesmärke ära kasutada, kui ettevõtted üritavad nõusoleku eesmärgi alla seada ka muid töötlemise toiminguid, mille kohta tegelikult nõusolekut pole võetud. Nõusolek kaotab oma mõtte, kui selle alla üritatakse sobitada olukordi, milleks seda ei kavatsetud kasutada. Seega tuleb uue eesmärgi puhul küsida uus nõusolek.

Näiteks annab jõusaali pidav ettevõte liikmetele võimaluse nõustuda e-kirjade saatmisega nõuannetega, kuidas selleks suveks vormi saada. Kuna selline nõusolek on seotud teatud ajalise

[279] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 20.
[280] Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679, p 20.

piiranguga ehk kuni suveni, siis on andmesubjekti ootus, et vastavaid kirju enam pärast suve ei saadeta.[281] Järelikult nõusolek peaks kehtima suveni.

Vanema nõusoleku puhul lapsele infoühiskonnateenuse pakkumisel on vanema nõusoleku kehtivus seotud lapse vanusega. Nimelt on vanema nõusolekut vaja üksnes juhul kui laps on alla 16-aasta vanune (art 8 lg 1). Seega kehtib vanema nõusolek senikaua kuni laps jõuab vanusesse, mil ta on õigustatud ise sellist nõusolekut andma.[282] Eelnev kehtib juhul kui nõusoleku võtmisel pole sätestatud muid ajalisi piiranguid nii nagu näiteks eelmise näite puhul. See loob ettevõtetele vajaduse järgida, millal laps jõuab sellisesse vanusesse, mil vanema nõusolekut pole enam vaja, mis tähendab spetsiaalse süsteemi loomise vajadust.

Kehtiva IKS-i kohaselt võib ettevõte tugineda andmesubjekti nõusoleku kehtivusele tema eluajal ja 30 aastat pärast andmesubjekti surma, v.a. juhul kui andmesubjekt pole teisiti otsustanud (IKS § 12 lg 6). Samuti ei saa andmesubjekti nõusolekule tugineda pärast seda, kui andmesubjekt on nõusoleku tagasi võtnud. Seda muidugi välja arvatud juhtudel, kui nõusolek on seotud justkui ühekordse töötlemise eesmärgiga.

Erinevalt andmekaitse määruses sätestatust näeb aga 2018. a. IKS-i eelnõu § 14 lõige 3 sarnaselt varem kehtinud õigusega ette, et andmesubjekti nõusolek kehtib andmesubjekti eluajal ja 30 aastat pärast andmesubjekti surma, kui andmesubjekt ei ole otsustanud teisiti. Liikmesriikidele on jäetud õigus seada eeskirju surnuid puudutavate isikuandmete töötlemiseks. Nõusoleku kehtivuse tähtaja seadmine isiku eluajal ei kuulu otseselt surnuid puudutavate isikuandmete töötlemise küsimuse alla. Samas ei tohiks sellise ajalise kehtivuse sätestamine olla vastuolus andmekaitse määruse põhjal selgitatut arvesse võttes. Kui nõusolek on antud kehtivalt ja töötlemine pole lõppenud, siis võibki nõusolekule tugineda andmesubjekti elu ajal. Samas on jäetud võimalus ka teistsuguste kokkulepete jaoks. Järelikult ei muutu ettevõtete jaoks nõusoleku ajalise kehtivuse põhimõtted.

3.8.2. Enne andmekaitse määrust antud nõusolekute kehtivus

Seni on käesolevas peatükis käsitletud nõudeid, kuidas võtta nõusolek tulevikus andmekaitse määruse nõuetele vastavalt ning millised on muutused seonduvalt kehtiva regulatsiooniga. Teisalt on oluline on ka välja selgitada, millistel tingimustel jäävad varasemad nõusolekud kehtima.

[281] Information Commissioner's office. Consultation: GDPR consent guidance, p 25.
[282] *Ibid*, p 26.

Andmekaitse määrus näeb ette, et andmesubjektil ei ole vaja oma nõusolekut uuesti anda, kui nõusoleku andmise viis on kooskõlas andmekaitse määruse tingimustega (preambula punkt 171). Selline lähenemine võib muuta paljud vanade andmekaitse-eeskirjade alusel kogutud nõusolekud kehtetuks. Eelnevalt on tuvastatud, et kuigi andmekaitse määrus seab uusi põhimõtteid, mis varasemalt pole IKS-is käsitletud, ei tähenda see koheselt seda, et varasemad nõusolekud oleksid kehtetud, kuna on võimalik, et kaudselt on nendega siiski arvestatud. Näiteks nagu tuvastatud läbipaistvuse põhimõtte puhul.[283] Seega peamiselt seab selline nõue raskusse ettevõtted, kellele oli isikuandmete töötlemisel ette nähtud mõned erandid.

Nõusoleku kehtetus võib siiski tulla kõne alla juhtudel, kus nõusolekud peavad vastama selgesõnalisuse nõudele[284] või seadusandja on lubanud võtta nõusoleku tüüptingimustes. Eelnevalt on leitud, et andmekaitse määruse alusel ei vasta tüüptingimustes võetud nõusolek määruse nõuetele.[285] Seni jäetud paljudes olukordades eriseadustega võimalus üldreeglist erandi tegemiseks, mille puhul ettevõtted ei pea nõusolekut võtma IKS-i nõudeid järgides. Näiteks on sellisteks seadusteks elektroonilise side seadus,[286] krediidiasutuste seadus, kindlustustegevuse seadus ja paljud muud seadused.[287] Krediidiasutuste seaduses on (edaspidi KAS) erisäte, mille kohaselt krediidiasutus võib nõusoleku võtta tüüptingimustes (KAS § 89 lõike 2^2). Selline säte lisati seadusesse 01.01.2008.[288] Samuti ei näe andmekaitse määrus ette võimalust nõusoleku regulatsiooni siseriikliku õigusega täpsustada.

Eelnevast tekib küsimus, kas seni seadustes sätestatud tüüptingimustes nõusoleku võtmise erand tuleb kehtetuks tunnistada. Ülimuslikkuse põhimõttest tuleneb, et siseriiklik norm tuleb jätta rakendamata siseriikliku ja Euroopa Ühenduse normi vastuolu korral, mida ei saa tõlgendamise kaudu lahendada. Sellisel juhul on Euroopa Ühenduse normil eelis ja seda rakendatakse siseriikliku normi asemel.[289] Seetõttu tunnistatakse IKS-i rakendamise seaduse eelnõuga eelnevalt välja toodud tüüptingimusi sisaldavad sätted kehtetuks.[290]

Määrusest tulenev nõue, mille kohaselt varasemad nõusolekud peavad vastama uutele nõuetele põhjustab ulatusliku varasemate nõusolekute kehtetuse. Loodud on olukord, kus paljude ettevõtete jaoks muutuvad nõusolekud tühiseks. Seega tuleks näiteks krediidiasutustel küsida

[283] Vt. ptk 3.3.2.3.
[284] Vt. ptk 3.5.
[285] Vt. ptk 3.3.2.2.
[286] Elektroonilise side seadus. RT I, 01.07.2017, 2.
[287] Isikuandmete kaitse seaduse seletuskiri. 1026 SE, lk 10.
[288] Krediidiasutuste seadus. RT I 1999, 23, 349, 01.01.2008.
[289] R. Eerola; T. Mylly; P. Saarinen. Euroopa Liidu õiguse alused. Tartu: Tartu Ülikooli Kirjastus 2001. Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. 4. täiend. vlj. Tallinn: Juura 2017, lk 92.
[290] Isikuandmete kaitse seaduse rakendamise seadus. Eelnõu 23.03.2018, §-d 31 ja 39. Kättesaadav: http://eelnoud.valitsus.ee/main#Fkf86wSO.

klientidelt uued nõusolekud nendel juhtudel, mil töötlemine põhines andmesubjekti nõusolekul, mis oli võetud tüüptingimustes.

Seadusandja on andmekaitse määruse loomisega tekitanud olukorra, kus ettevõte ei saa olla kindel kehtestatud normide püsimajäämise suhtes, kuna määrusega peavad nõusolekud vastama uutele nõuetele. Sellises olukorras võib olla tegemist ettevõtlusvabaduse piiramisega. Kuigi ettevõtlusvabaduse õigus ei tulene otseselt EIÕK-st, on EIK neid piiranguid siiski tunnistanud EIÕK 1. lisaprotokolli artiklis 1 omandi segamatu kasutamise õiguse riivena ning hinnanud sellest aspektist ka riive põhjendatust.[291] Küll on aga ettevõtlusvabadust tunnustatud Euroopa Liidu põhiõiguste harta artiklis 16, mille kohaselt tunnustatakse ettevõtlusvabadust ühenduse õiguse ning siseriiklike õigusaktide ja tavade kohaselt. Kuivõrd tegemist on komplekse teemaga, mis vajab eraldi põhjalikumat analüüsi, ei lange see käesoleva töö uurimisobjekti alla.

Andmekaitse määrusest tulenevat nõuet, mille kohaselt varasemad nõusolekud peavad vastama uutele, on ka palju kritiseeritud. Nimelt leitakse, et andmekaitse määrusele eelnevate nõusolekute alusel töötlemine, mis vastab andmekaitse direktiivi ja liikmesriigi õigusele, peaks olema lubatud senikaua kuni töötlemise eesmärgid ei muutu.[292] Vastasel juhul võib tekkida olukord, kus ettevõtted ei saa enam klientidele pakkumisi saata, kuigi nad on sellega nõustunud, ning see võib mõjutada majandust. Teisalt võib see kaasa tuua ettevõtete meeleheitliku püüde saada klientidelt uued nõusolekud. Seega võidakse kliendile e-poe külastamisel sisse logitud keskkonnas peale suruda nõusoleku vormi, millest ei saa enne mööda minna, kui klient teeb kas nõustumise või mittenõustumise valiku.

Siiski tuleb välja tuua, et varasemate nõusolekute mitte vastavus ei muuda kõiki töötlemise toiminguid tagasiulatuvalt õigusvastaseks, kuna andmekaitse määrus ei oma tagasiulatuvat jõudu.

Välistatud ei ole olukord, et ettevõtted leiavad oma protsesse üle vaadates, et töötlemise jaoks peaks olema nõusoleku asemel hoopis muu andmekaitse määruse artiklis 6 sätestatud alus. Peatükis 3.6. on selgitatud, et kui juba töötlemise käigus on selgunud, et kohaldamisele sobiks uus õiguslik alus ning seda alust saab õiguspäraselt kohaldada, siis võib töötlemine jätkuda.[293] Seega võivad ettevõtted juhul, kui töötlemise ajal selgub, et varasem nõusolek ei vasta määruse nõuetele, tugineda muule õiguslikule alusele, kui selle kehtivuse eeldused on täidetud. See

[291] O. Kask, S. A. Ehrlich, *A.* Henberg. Põhiseaduse § 31 kommentaar, komm 3. – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017.
[292] Centre for Information Policy Leadership. Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Consent", p 24.
[293] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, p 13.

vähendab ettevõtete koormust hakata andmesubjektidelt uusi nõusolekuid küsima, kui õiguslik alus töötlemiseks pole tegelikult nõusolek.

Kui töötlemine on lõpetatud, andmed kustutatud või esineb mõni muu õiguslik alus andmete töötlemiseks, pole nõusolek enam vajalik. Vastasel juhul tuleb küsida uus nõusolek, mis vastab määruse eeskirjadele.

Kokkuvõtlikult on andmekaitse määruse nõue, mille kohaselt kõik nõusolekud peavad vastama uutele nõuetele, ebamõistlik. Mõistlikum oleks määruse nõuetele üleminek tagada nii, et uutele nõuetele peavad vastama uued nõusolekud.

KOKKUVÕTE

Töö põhieesmärk oli teha kindlaks, millistel juhtudel on ettevõtetel isikuandmete töötlemiseks vaja andmesubjekti nõusolekut ning kas andmekaitse määrusest tulenevad nõusoleku nõuded muudavad ettevõtetele kehtiva nõusoleku saamise raskemaks. Töö eesmärgiga seondub Euroopa Komisjoni soov tagada andmekaitse määrusega üksikisikute õiguste parem kaitse.

Töö esimeses peatükis käsitleti, mis hetkest hakati rääkima nõusoleku alusel isikuandmete töötlemisest, kuidas on nõusoleku mõiste kujunenud ning kuidas on see kajastatud õigusaktides.

Nõusoleku alusel hakati isikuandmete töötlemisest rääkima OECD 1980. aasta juhendis. Kuigi juhend määratles esimest korda rahvusvahelisel tasandil ära isikuandmete töötlemise õiguslikud alused, polnud need põhimõtted siiski liikmesriikidele siduvad. Euroopa liidu liikmeriikidele muutusid isikuandmete töötlemise alused kohustuslikuks 1995. aastal, kui võeti vastu andmekaitse direktiiv. Andmekaitse direktiiv oli Euroopa isikuandmete kaitse olulisim alusdokument, mis määratles ära töötlemise õiguslikud alused. Kuna OECD juhend oli direktiivi väljatöötamise aluseks, kandus direktiivi üle põhimõte, mille kohaselt isikuandmete töötlemine on muuhulgas lubatud andmesubjekti nõusolekul. Andmesubjekti nõusolek tähendas direktiivis iga vabatahtlikku, konkreetset ja teadlikku tahteavaldust, millega andmesubjekt annab nõusoleku töödelda tema kohta käivaid andmeid. Lisaks tulenes andmekaitse määruse artikli 7 punktist a, et nõusolek tuleb anda ühemõtteliselt.

Eesti õiguses oli enne IKS-i kehtestamist isikuandmete kaitse reguleeritud Põhiseaduses, mis sätestas üldise kaitse eraelu puutumatusele, mis hõlmas isikuandmete kaitset. Nõusoleku vajadusest isikuandmete töötlemisel hakati rääkima 1996. aastal, kui kehtestati IKS ning nõusoleku alusel töötlemine on isikuandmete kaitse regulatsiooni jäänud Eesti õigusesse tänaseni.

Nõusoleku mõiste on aja jooksul edasi arenenud ning muutunud üha täpsemaks. Nõusoleku esmakordsel sätestamisel rahvusvahelisel tasandil ei defineeritud nõusoleku mõistet. OECD juhendis oli nõusolek küll toodud välja isikuandmete töötlemise õigusliku alusena, kui juhendis ei täpsustatud nõusoleku definitsiooni. Esimest korda anti nõusolekule definitsioon andmekaitse direktiivis, mille kohaselt nõusolek on iga vabatahtlik, konkreetne ja teadlik tahteavaldus, millega andmesubjekt annab nõusoleku töödelda tema kohta käivaid andmeid.

Eesti õiguses oli 1996. aasta IKS-is nõusolek defineeritud kui selgelt väljendatud tahteavaldus, millega isik lubab oma isikuandmete töötlemist pärast seda, kui teda on teavitatud isikuandmete töötlemise eesmärgist ja õiguslikust alusest, isikuandmete koosseisust ja allikast, kolmandatest isikutest või nende kategooriatest, kellele isikuandmete üleandmine on lubatud, üldiseks

kasutamiseks antavate isikuandmete loetelust, vastutava töötleja või tema esindaja nimest ja aadressist. Sellega oli nõusoleku definitsioonis ühendatud ka teave, mida oli vaja andmesubjektile nõusoleku andmiseks anda.

2004. aasta IKS-is hakati selgelt nõusoleku definitsiooni ja edastamiseks vajalikku teavet eristama. Nõusoleku definitsioon säilitas oma varasema tähenduse, kuid isikuandmete töötlejale seati uusi kohustusi, millest isikuandmete töötleja peab andmesubjekti teavitama. Näiteks peab teavitama andmesubjekti õigusest nõuda isikuandmete töötlemise lõpetamist ning isikuandmete parandamist, sulgemist, kustutamist ja peab teavitama, millal andmesubjektil on õigus saada juurdepääs tema kohta töödeldavatele isikuandmetele. Samuti seati nõusolekule kehtivusaeg ning tõendamiskoormis töötlejale, mille kohaselt ta peab suutma tõendada, et andmesubjekt on nõusoleku andnud.

2008. aasta muudatusega muudeti isikuandmete definitsiooni. Kehtima jäi põhimõte, mille kohaselt nõusolek on andmesubjekti tahteavaldus, millega ta lubab oma isikuandmeid töödelda. Samuti on lisatud, et see kehtib üksnes juhul, kui see tugineb andmesubjekti vabal tahtel. Nõusolekut võis anda osaliselt ja tingimuslikult.

Eelnevat definitsiooni võrreldi käesolevas töös andmekaitse nõuetega. Andmekaitse määruses tähendab nõusolek andmesubjekti vabatahtlikku, konkreetset, teadlikku ja ühemõttelist tahteavaldust, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega.

Ainuüksi sõnastusest tulenevalt jagab andmekaitse määrus nõusoleku definitsioonis nõusolekule konkreetsed nõuded, mida IKS pole sõnaselgelt teinud. Seega tuli võrrelda, milliseid muudatusi toob see kaasa ka sisuliselt. Enne seda aga kontrollis autor, milliseid muudatusi toob kaasa õiguslike aluste muutus andmekaitse määruses, et selgitada, millal on isikuandmete töötlemiseks vaja andmesubjekti nõusolekut.

Töö teises peatükis käsitleti, millal on andmekaitse määruse alusel vaja nõusolekut küsida ning kuidas seda eristada teistest õiguslikest alustest. Samuti uuriti nõusoleku küsimise vajaduse muutumist võrreldes seni kehtinud regulatsiooniga.

Andmekaitse määruse alusel on andmesubjekti nõusolekut vaja juhtudel, kui ükski teine määruses toodud õiguslik alus kohaldumiseks ei sobi. Seega on ettevõttel vaja tugineda nõusolekule, kui isikuandmete töötlemise aluseks ei sobi andmesubjekti taotlus, leping, seadus, elu ja tervise kaitse vajadus või õigustatud huvi. Oluline on erinevaid õiguslike aluseid eristada,

kuna töötleja võib valida ainult ühe aluse ning ei või töötlemise kestel õiguslike aluseid vahetada.

Nõusoleku alusel töötlemise üldpõhimõte on, et nõusolekut on vaja iga töötlemise eesmärgi jaoks eraldi. Kui isikuandmete töötlemise eesmärk ajas muutub, on isikuandmete töötlejal vaja uut nõusolekut.

Samas on autor leidnud, et kui eesmärke saab ühendada, võib töötleja küsida ühe nõusoleku mitme asemel. Töö käigus selgus, et töötlemise eesmärkide muutumisel pole vaja uut nõusolekut juhul, kui andmesubjekt võis sellisel eesmärgil töötlemist mõistlikult eeldada.

Lisaks eelnevale on andmekaitse määruse alusel isikuandmete töötlemiseks vaja nõusolekut infoühiskonnateenuse pakkumisel lapsele, eriliigiliste isikuandmete töötlemisel, isikuandmete edastamisel kolmandale riigile või rahvusvahelisele organisatsioonile, kui sellega pole tagatud piisav kaitse ja automatiseeritud otsuste puhul.

Täiendava probleemkohana käsitleti töös nõusoleku vajadust otseturunduspakkumiste saatmisel. Kuigi nõusoleku vajadus otseturunduspakkumisteks ei tulene otse andmekaitse määrusest, siis õiguskirjanduses põhinevad paljud käsitlused nõusoleku nõuete hindamisel otseturundusel, mistõttu nägi töö autor vajadust selgitada nõusoleku alusel töötlemist otseturunduse puhul. Õigustatud huvile saab ettevõte tugineda pakkumiste saatmisel juhul, kui pakkumine ei erine teenusest või toodetest, mida klient on ettevõttes tarbinud ning kontaktandmed on kogutud teenuse osutamise käigus. Samas pakkumised muude toodete kohta, mida klient pole ettevõttelt ostnud, väljuvad õigustatud huvi raamidest ning selleks on vaja kliendi nõusolekut.

Töös selgus, et nõusoleku eristamisel seaduse, eluliste huvide kaitseks, avaliku huvi alusel ja automatiseeritud töötluseks ei tekita niivõrd olulist kahtlust õige õigusliku aluse valimises. Nõusoleku eristamine on põhiliselt problemaatiline lepingu alusel töötlemisest, kuna praktikas võidakse eksida, kas töötlemine toimub lepingu või nõusoleku alusel. Andmekaitse määruse tõlgendamisel on õiguskirjanduses siiski asutud seisukohale, et enne tuleks vaadata, kas töötlemine võiks toimuda lepingu alusel ning alles seejärel kontrollida õigusliku aluse vajaduseks nõusolekut.

Lisaks annab andmekaitse määrus juurde kaks uut õigusliku alust - töötlemine andmesubjekti taotluse alusel ning samuti lubab määrus varasemalt ulatuslikumalt tugineda õigustatud huvile. Uute aluste kaasatoomine vähendab praktikas nõusoleku vajadust. Autori hinnangul toetavad nõusoleku vajaduse vähenemist mõlemad uued õiguslikud alused. Kui enne võisid ettevõtted

praktikas tugineda taotluse esitamisel isikuandmete töötlemisel nõusolekule, siis määruse jõustumisega on töötlemise aluseks andmesubjekti taotlus. Isikuandmete töötlemisel õigustatud huvi osas väheneb nõusoleku vajadus otseturundusega seonduvalt pakkumiste saatmisel, mis seonduvad kliendi tarbitud toodete ja teenustega. Kuna eelnevalt sellised alused puudusid, sai töötlemine toimuda andmesubjekti nõusolekul.

Töö kolmandas peatükis käsitleti andmekaitse määrusest tulenevaid nõusoleku tingimusi ning uue regulatsiooniga kaasnevaid muutusi võrreldes kehtiva regulatsiooniga.

Andmekaitse määrus sätestab täpsemad tingimused, mida on kehtiva nõusoleku saamiseks vajalik täita. Määruse kohaselt peab nõusolek olema vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljenduva tegevusega nõustub tema kohta käivate isikuandmete töötlemisega. Töös kontrolliti, kas ja milline element nõusoleku küsimisel muutub võrreldes varasemaga.

Töös on leitud, et IKS-is sisaldub juba täna vabatahtlikkuse põhimõte. Siiski pole Eesti õiguskirjanduses ja kohtupraktikas vabatahtlikkust põhjalikult lahti kirjeldatud nii nagu seda on tehtud andmekaitse määruse puhul, mistõttu määrus täpsustab vabatahtlikkuse elemente.

Ühe uue nõudena sätestab andmekaitse määrus konkreetsuse põhimõtte. Konkreetsuse nõue näeb ette, et nõusoleku küsimisel peab töötleja tooma välja töötlemise konkreetsed eesmärgid. See põhimõte on haakuv ka mitme teise põhimõttega, näiteks jaotatavuse põhimõttega, mille kohaselt nõusolek tuleb küsida iga andmete töötlemise eesmärgi jaoks eraldi. Täna kehtivas IKS-is ega õiguskirjanduses ei selgitata, millise detailsuse astmega peab eesmärke eristama. Eesti õigusest tuleneb üksnes, et andmesubjektil endal on võimalus eesmärke eristada ja anda nõusolek üksnes osaliselt. Seega seab määrus selgemad piirid, kui täpne peab nõusolek olema ning milliste eesmärkidega seotud.

Teisalt on töö autor järeldanud, et kui eesmärgid on ühendatavad ning andmesubjekt võib mõistlikult mingil viisil isikuandmete töötlemist oodata, pole isiku koormamine erinevate nõusolekutega mõistlik, mistõttu võib andmesubjektilt küsida ühe nõusoleku. Kui eesmärk on ajas muutunud, siis pole uut nõusolekut vaja, kui uus töötlemise eesmärk on kooskõlas esialgsega. Töös on leitud, et andmesubjektile e-kirja saatmine nõusoleku valikute uuendamiseks vajab siiski andmesubjekti nõusolekut.

Lisaks sätestab andmekaitse määrus ranged nõuded nõusoleku andmisele infoühiskonnateenuse pakkumisel. Ettevõtte jaoks muutub keerulisemaks eri liikmesriikides tegutsedes iga riigi nõuete eraldi kindlaks tegemine ja süsteemide ülesehitamine selleks, et eristada, mis vanusest

saab laps ise anda nõusoleku. Samuti tuleb teenuse pakkumiseks saada vanema nõusolek, mis teeb taaskord keeruliseks tõendamise, et teisel pool ekraani oli nõusoleku andjaks vanem.

Nõusoleku küsimisel on oluline osa kohustuslikul teabel, mida peab andmesubjektile enne nõusoleku andmist esitama. Kehtiv regulatsioon erineb aga andmekaitse määrusest selles osas, et määrus eristab nõusolekut ja nõusoleku küsimiseks esitatavat teavet aga IKS-i järgi moodustab kohustuslik informatsioon justkui nõusoleku osa. Seega võis IKS-i alusel olla nõusolek kohe tühine, kui nõusolekust oli oluline teave välja jäänud. Kuna andmekaitse määruse alusel on teadlikkus nõusoleku üheks eeltingimuseks, võib ka määruse alusel teabekohustuse rikkumine tuua kaasa nõusoleku tühisuse ning rahatrahvi, kui esitamata jäeti teave, mis peab olema nõusoleku juures.

Nõusoleku juures esitatava teabe juures tuleb reeglina andmesubjekti teavitada kes, milleks ja millisel alusel tema isikuandmeid töötleb. Lisaks teabele, mis tuleb andmesubjektile edastada kohe, tuleb eristada ka teavet, mis tuleb andmesubjektile edastada hiljemalt ühe kuu jooksul nõusoleku andmisest. Selle võib edastada näiteks ettevõtte veebilehekülje asuva privaatsuspoliitika kaudu. Kuna ka Eesti õiguses on seadus ja praktika soodustanud privaatsuspoliitikate kasutamist, ei kaasne määrusega nõudeid, mille kohaselt kogu teabe peaks esitama nõusoleku juures.

Teisalt suureneb esitatava teabe maht. Võrreldes IKSi-ga on isikuandmete töötlejal uuena kohustus teavitada andmesubjekti isikuandmete töötleja ja andmekaitseametniku kontaktandmetest, isikuandmete säilitamise ajavahemikust või säilitamise kriteeriumitest, töötleja õigustatud huvist ning õigusest võtta nõusolek tagasi.

Andmekaitse määruse alusel tuleb teave edastada kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt. Eesti õiguskirjanduses pole teabe esitamise nõudeid nii põhjalikult lahti selgitatud. Ehkki tegemist on nõuetega, mille peale võiks mõistlikult ettevõte ka ise tulla, siis võttes arvesse, et nõuetega mittevastavuses olemine võib kaasa tuua suure rahatrahvi, ei saa ettevõtted endale sellist riski lubada. Järelikult suureneb teabele esitatavate nõuete järgimise kohustus.

Ühe uue põhimõttena seab määrus läbipaistvuse põhimõtte, mida Eestis pole isikuandmete kaitse regulatsioon varasemalt käsitlenud. Läbipaistvuse põhimõte aitab selgitada, kuidas teavet tuleb edastada. Selleks peab teave ja sõnumid olema lihtsalt kättesaadavad, arusaadavad, selgelt ja lihtsalt sõnastatud, korrektne ja terviklik. Vajadusel võib teabe edastada liikuva pildi abil. Samas kattub läbipaistvuse põhimõte üldiselt teabe kättesaadavusele seatud nõuetega, mistõttu

ei too see põhimõte kaasa olulist muudatust, kui teabe edastamisel võetakse arvesse juba kõiki eelnevalt käsitletud kriteeriume.

Töös on leitud, et nõusoleku nõuete järgimisel võib ettevõtetel tekkida raskusi selgesõnalise nõusoleku küsimisel, kuna määrusest ei tulene, mida selgesõnalisus tähendab. Töö käigus selgus, et andmekaitse määrus peidab selgesõnalisuse nõude taga vorminõuet. Ühest küljest on nõusolek selgesõnaline, kui see on antud kirjalikult, teisest küljest vastab see selgesõnalisuse nõuetele, kui nõusolek on antud kahe-etapilise kinnitusena, kusjuures kinnitus tuleb esitada samuti vähemalt kirjaliku taasesitamist võimaldavas vormis. Andmekaitse määruse väljatöötamisel võis olla sellise nõude tagamõte olla mõnevõrra paindlikkuse kehtestamine, et mitte nõuda osadel juhtudel nõusolekut kirjalikult. Praktikas võib selgesõnalisus nõue ettevõtteid eksitada, kuna määrus ise ei selgita, mida selle nõude all tegelikult mõeldakse ning kuidas neid nõudeid täita. Kõige turvalisem oleks lähtuda kirjalikust nõusolekust, kuna sellega garanteerib ettevõte, et nõusolek on antud selgesõnaliselt ning sellega on olemas ka tõend nõusoleku kohta.

Lisaks andmekaitse määrusele, täpsustab ka uus isikuandmete kaitse seadus nõusoleku nõudeid ulatuses, milles see õigus on liikmesriikidele jäetud. Näiteks lahendab 2018. a. IKS-i eelnõu erandite kehtestamisega, mil nõusolekut pole vaja, mõningad seni kehtivas regulatsioonis olnud probleemid. Kui varasemalt oli kirjanduse tarbeks isikuandmete töötlemisel vaja andmesubjekti nõusolekut, siis 2018. a. IKS-i eelnõu kohaselt nähakse ette erand, mil nõusolekut pole vaja. Seetõttu jäävad ära probleemid, mis varem tõusetusid näiteks nõusoleku tagasivõtmisega vahetult enne isikute kohta tehtud filmi linastumist.

Täiendav küsimus tekkis töös seoses vorminõude puudumisega. Nimelt ei näe andmekaitse määrus ette vorminõuet. Nõusoleku ühemõttelisuse all on selgitatud, et nõusoleku võib anda ka selget nõustumist väljendava tegevusega. Eesti seni kehtinud õigus aga ei võimalda nõusolekut anda suuliselt, välja arvatud juhul, kui vorminõude järgmine ei ole andmetöötluse erilise viisi tõttu võimalik. Järelikult annab andmekaitse määrus justkui vabastuse seni kehtinud vorminõudest. Autor leidis, kuna isikuandmete töötleja peab olema võimeline tõendama kehtiva nõusoleku andmist andmesubjekti poolt, ei oma vorminõude kaotamine sisulist mõju nõusoleku regulatsiooni lihtsustamisel. Seega tõendamiseks oleks vajalik siiski küsida nõusolek vähemalt kirjalikku taasesitamist võimaldavas vormis.

Lisaks on andmekaitse määrus loonud täiendava probleemi varasemate nõusolekutega. Kui varasemad nõusolekud ei vasta uute nõusoleku nõuete tingimustele, pole nõusolek kehtiv. Seega muutuvad kehtetuks nõusolekud, mis olid lubatud eriseadusega, näiteks krediidiasutuste

seaduses, võtta tüüptingimustes. Kuna andmekaitse määrus eristab nõusolekut ja selleks esitatavat teavet, siis asjaolu, et määrusega kaasneb täiendav teabe esitamise kohutus ei mõjuta varasemate nõusolekute kehtivust.

Andmekaitse määrus on pannud paljud ettevõtted isikuandmete töötlemisega seonduvaid protsesse ja töötlemise aluseid üle hindama, et mitte olla vastuolus andmekaitse määrusega. Autori arvates pole sellises mahus protsesside üle vaatamist Eestis isikuandmete töötlemise valguses toimunud vähemalt viimase isikuandmete kaitse regulatsiooni jõustumisest alates ehk 10 aastat.[294] Autori hinnangul pole tegutsema pannud mitte üksnes soov olla isikuandmete jõustuva regulatsiooniga vastavuses, vaid ka hirm hiigeltrahvide ees.

Nagu töös selgus, on isikuandmete töötlemise õiguslike aluste ülevaatamiseks ka põhjust. Kuigi andmekaitse määrus vähendab nõusoleku vajadust, siis samas karmistuvad mõnevõrra reeglid, kuidas nõusolekut peab andma. Nii muutuvad andmekaitse määruse jõustumisel mitmed olulised küsimused töös käsitletud nõusoleku regulatsiooni osas – konkreetsus, teadlikkus, ühemõttelisus, selgesõnalisus ja nõusoleku vorm.

Kehtiv IKS täna juba sisaldab paljuski andmekaitse määrusest tulenevaid nõusoleku nõudeid. Samas on andmekaitse määrus kohati oma sõnastusega tekitanud siiski olukorra, kus ettevõtetel on keeruline üksnes määruse nõudeid järgides saada aru, millistele nõuetele peab nõusolek vastama, näiteks selgesõnalisuse juures. Järelikult muudab andmekaitse määrus ettevõtetel kehtiva nõusoleku saamise osaliselt raskemaks. Teisalt annab vorminõude puudumise tõttu võimaluse küsida nõusolek ka muul viisil kui kirjalikult, kui seda annab hiljem tõendada.

Nõusoleku valimisel õiguslikuks aluseks ja selle nõuete täitmisel tuleb lähtuda siiski põhimõttest, et kui ettevõttel tekib raskusi nõusoleku vastavusse viimisega kõikidele eeltoodud nõuetele, on tegemist märgiga, et nõusolek ei pruugi olla töötlemiseks kõige õigem alus. Seega tuleb kahtluse korral vaadata, ega mõni teine alus ei sobiks paremini isikuandmete töötlemise õigustamiseks.

[294] Kehtiv isikuandmete kaitse seadus jõustus 01.01.2008.

The necessity and conditions of consent from General Data Protection Regulation for processing of personal data by companies. Summary

Personal data has become very valuable in the 21st century, which is why it has even been called the good of the 21st century. The amount of data processed by computers doubles every two years. Cloud computing has evolved, in which individuals record sensitive personal data on someone else's servers, thus losing control over it. The risks to privacy and the protection of personal data arising from online activities are increasing.

Data protection law must evolve, in order to come to grips with these new realities. According to the European Commission's assessment, the objectives and principles of the protection of personal data contained in the Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the Data Protection Directive) are still up-to-date. However, over the past twenty years, the rapid development of technology and globalization have created new challenges in the area of personal data protection. Therefore, it was necessary to thoroughly reform data protection regulation in order to strengthen the right to privacy in the Internet.

In the Commission’s view, the need for a new instrument is also due to the fact that, to date, Member States have not been able to fully align national law with the Directive. This has led to fragmentation, legal uncertainty and uneven implementation of the current data protection regulations in the Member States, which creates barriers to business and increases the administrative burden on the public sector.

On the initiative of the European Commission, a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data was adopted on 27 April 2016. The Data Protection Regulation does not change the principle that the processing of personal data may be based on the consent of the data subject, but the regulation clarifies the conditions that companies must comply with in order to obtain the true consent of the data subject.

In order to implement the new regulation, at the time of writing, a new draft Personal Data Protection Act has been submitted to the Parliament by the Government of the Republic of Estonia.

The main purpose of this thesis was to determine in which cases the data subject's consent is required for the processing of personal data by enterprises. The main aim of the thesis was to ascertain whether the consent requirements arising from the Data Protection Regulation makes

it harder for enterprises to obtain valid consent in the Estonian legal environment. To achieve the goal, the need and conditions for consent are assessed in relation to the current personal data protection regulation.

In accordance with the set goal, the structure of the thesis was developed. The thesis was divided into three chapters. The first part of the thesis dealt with the history of the formation of a claim for consent as the legal basis for the processing of personal data. The chapter introduced legislation that gave rise to the protection of personal data and the legislation which are based on the consent to justify the processing of personal data. The first chapter addressed the issue from which period there were discussions about the processing of personal data on the basis of consent, how the concept of consent has developed and how has this been reflected in the legislation.

The second chapter of the thesis provided an overview of the cases of need for consent under the Data Protection Regulation. The second chapter seeked to answer the question of when the data protection regulation requires consent and how to distinguish it from other legal bases. The second chapter also dealt with the changes to the need to ask for consent as compared to the current regulation.

The third chapter dealt with the terms of the consent. In the third chapter, the research question was raised about the conditions that must be met by the current consent, and what changes the new requirements bring with respect to the current regulation.

The first part of the thesis was based on the historical-chronological method. In the second and third parts of the thesis, answers to the research questions were achieved using a systematic, qualitative, analytical and comparative method. The purpose of the comparative method was to assess whether the Data Protection Regulation will result in more stringent requirements for consent as compared to the current Personal Data Protection Act in Estonia.

On role of consent in the processing of personal data was first emphasized in the 1980 OECD guidelines, but these principles were not binding to the Member States. The bases for processing personal data became mandatory in the Member States of the European Union in 1995 when the Data Protection Directive was adopted. The Data Protection Directive was the most important source of European personal data protection, defining the legal basis for processing. The Data Protection Directive has transposed the principle that personal data could be processed on the basis of consent.

In Estonian law, prior to the introduction of the Personal Data Protection Act (hereinafter PDPA), personal data protection was regulated by the Constitution, which provided for the general protection of privacy, which included the protection of personal data. The need for consent for the processing of personal data began to be spoken of in 1996 when the PDPA was introduced. The processing of consent has been subject to the protection of personal data protection in Estonia ever since. Over time, the definition of consent in the PDPA has evolved, and today, a consent, i.e. the declaration of intention of a data subject whereby the person permits the processing of his or her personal data (hereinafter consent) is valid only if it is based on the free will of the data subject.

The definition of consent in the PDPA has been compared with the requirements for consent in the Data Protection Regulation. In the Data Protection Regulation, consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Based solely on the wording, the Data Protection Regulation provides for specific requirements to consent that are not explicitly stated in the PDPA. Therefore, it was necessary to compare what changes this entails.

According to the Data Protection Regulation, the consent of the data subject is required in cases where none of the other legal bases set out in the Regulation is appropriate. Therefore, a company needs to rely on consent if the data subject's request, contract, law, the need for protection of life and health or legitimate interest is not the correct basis of the processing of personal data.

The general principle of processing under consent is that consent is needed for each processing purpose individually. If the purpose of the processing of personal data changes in time, the processor of personal data needs a new consent. However, the author has found that if the goals can be combined, the processor can ask for only one consent for several of these combined goals. The thesis revealed that there is no need for new consent in the event of a change in the purpose of the processing, if the data subject could reasonably have expected the processing for such purpose.

In addition to the above, the processing of personal data under the Data Protection Regulation requires consent for the provision of an information society service to a child, the processing of personal data of a specific type, the transfer of personal data to a third country or an international organization, provided that it does not provide adequate protection and for automated decisions.

The consent for direct marketing offerings is required if the company makes offers for products that the customer has not purchased previously from the company. Otherwise the correct legal basis is legitimate interest.

The Data Protection Regulation sets out two new legal bases for the processing of personal data, compared to the PDPA - the request of the data subject and it also allows to rely on legitimate interest more extensively. The new legal bases will, in practice, reduce the need for consent, since such processing could have until now taken place only based on consent.

As regards the conditions of consent, the Data Protection Regulation sets out more precise conditions that must be met to obtain valid a consent. In the thesis it was analysed if and when the request for consent changes as compared to the previous regulation.

The author concluded that the principle of freely given consent is included in the PDPA today. However, in Estonian legal literature and case-law, freely given consent has not described in detail as it has been done with the Data Protection Regulation. Therefore, the Data Protection Regulation explains the optional elements of the regulation.

As one of the new requirements, the Data Protection Regulation sets out the principle of specificity which means that the consent shall be specific and connected to certain predefined objectives.

The author of the thesis has concluded that if the goals are interconnected and the data subject can reasonably expect some kind of processing of personal data, it is not reasonable to encumber the data subject with numerous requests for consent. Rather, a single request for consent is appropriate in such a situation. If the goal has changed in time, then no new consent is required if the new processing objective is consistent with the original.

Under the Data Protection Regulation, for companies, it becomes more difficult to provide information society services to children, as it becomes more complicated for the company to work in different Member States, having to identify each country's requirements separately and building up systems to differentiate by which age the child can give consent. A parental consent must also be obtained to provide the service, which once again makes it difficult to prove that the consent was indeed given by the parent.

The Data Protection Regulation also extends information that must be presented with the consent. Compared to the PDPA, the controller of the personal data is newly obliged to inform the data subject about the contact details of the data controller and the data protection officer, the period of maintenance of the personal data or the criteria for its maintenance, the legitimate

interest of the controller and the right to withdraw. In addition, the regulation will specify how this information should be transmitted. The information must be communicated in a concise, clear, comprehensible and easily accessible format, using clear and simple language. PDPA did not foresee such requests for information. Although these are requirements that could reasonably be met by a company itself, considering that non-compliance can lead to a large fine, companies cannot afford such a risk, therefore raising the need for professional consultations.

One of the new principles of the Data Protection Regulation is transparency. At the same time, the principle of transparency is generally in line with the requirements for access to information, which means that this principle does not lead to a significant change if all the criteria previously addressed are already taken into account in the transmission of information.

Compliance with the requirements of consent may create difficulties while trying to ask for explicit consent, as the regulation does not give rise to what explicitly means. In the thesis, it became clear that the Data Protection Regulation hides a form requirement in the need for explicit consent. Consent is explicit if it is given in writing, but it also fulfils the requirements of explicitly in case consent is given as a two-step confirmation and the statement must also be submitted in at least a written reproducible format. According to the author, it would be most reasonable for companies to have a consent reproducible in writing, as it guarantees the company that the consent is explicitly issued and that there is also evidence of consent.

Although the Data Protection Regulation reduces the need for consent, the rules on how consent has to be given will somewhat tighten. Thus, when the Data Protection Regulation enters into force, a number of important issues raised in the current thesis will change, although the current PDPA already contains much of the consent requirements arising from the Data Protection Regulation.

KASUTATUD MATERJALID

Kasutatud kirjandus ja seaduseelnõud

1. Brink, S; Wolff, H. A. BeckOK Datenschutzrecht. 23. Auflage. München: Verlag C.H.BECK 2018.
2. Bussche, A; Voigt, P. Data protection in Germany: including EU General Data Protection Regulation. Berlin: Springer 2018.
3. Bussche, A; Voigt, P. The EU General Data Protection Regulation. A practical Guide. Springer: 2017.
4. Bygrace, L. A. Data Privacy Law. An International Perspctive. Oxford University Press 2014.
5. Carey, P. Data protection: a practical guide to UK and EU law. Oxford: Oxford University Press 2004.Data Protection Network. Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation. 10.07.2017. https://iapp.org/media/pdf/resource_center/DPN-Guidance-A4-Publication.pdf, 01.04.2018.
6. Eerola, R; Mylly, T; Saarinen, P. Euroopa Liidu õiguse alused. Tartu: Tartu Ülikooli Kirjastus 2001. Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. 4. täiend. vlj. Tallinn: Juura 2017.
7. Euroopa Komisjon. Ettepanek privaatsust ja elektroonilist sidet käsitlevale määrusele. Brüssel: 2017. Kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1506862238432&uri=CELEX:52017PC0010, 01.04.2018.
8. Euroopa Komisjon. Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus). Brüssel: 2012. Kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=COM:2012:0011:FIN, 01.04.2018.
9. European Commission. Special Eurobarometer 431. Data Protection Report. 2015. Available: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf, 01.04.2018.
10. Fink, E. Õiguspärase ootuse kaitse eeldused ja piirid Euroopa Liidu õiguses. Tartu Ülikooli Kirjastus 2016.
11. Fundamental Rights Agency, European Commission. Handbook on European Data Protection law. Luxemburg: Publications office of the European Union, 2014. Available: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, 01.04.2018.

12. Harari, Y. N. Homo Deus, A Brief History of Tomorrow. London: Harvill Secer 2016.
13. Henberg, A. Isikuandmete töötlemine töösuhtes. - Juridica 2005, nr 8.
14. Information Commissioner's Office. Consultation: GDPR consent guidance. London: 2017. Available: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf, 01.04.2018.
15. Isikuandmete kaitse seaduse eelnõu seletuskiri. 06.11.2017. Justiitsministeerium. Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_sk_9.11.17.pdf, 01.03.2018.
16. Isikuandmete kaitse seaduse seletuskiri. 1026 SE. Justiitsministeerium. – Kättesaadav: http://www.aki.ee/et/eraelu-kaitse/oigusaktid, 01.04.2018.
17. Isikuandmete kaitse seaduse seletuskiri. 2004. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/fda65853-f05c-3b4e-ad4f-27f017828fcd/Isikuandmete%20kaitse%20seadus, 01.04.2018.
18. ITGP Privacy Team. EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide. Ely: IT Governance Publishing 2017.
19. Kerikmäe, T. Euroopa Liit ja õigus. Tallinn: Õiguskirjastus 2000.
20. Kuner, C. European Data Privacy Law and Online Business. Oxford: Oxford University Press 2003.
21. Laffranque, J. Euroopa Liidu õigussüsteem ja Eesti õiguse koht selles. Tallinn: Juura 2006.
22. Lammerant, H; Hert, P. Data protection on the Move – current developments in ICTT and Privacy/DataProtection. Springer 2016.
23. Paal B. P.; Pauly, D. A. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz. Verlag C.H. Beck: 1. Auflage 2018.
24. Mikiver, M. Kes on tarbija kliendiandmete peremees? Otseturustus krediidiasutuste näitel. – Juridica 2015, IV.
25. Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011.
26. Tikk, E; Nõmper, A. Informatsioon ja õigus. Tallinn: Juura 2007.
27. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD 1980. Available: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, 01.04.2018.
28. Rondel, M. Informatsioonilise enesemääramise õigus ja jälitustegevus. Isiku õigus teada saada tema suhtes tehtud jälitustoimingutest. - Juridica 2016, nr 10.

29. Seletuskiri elektroonilise side seaduse ja infoühiskonna teenuse seaduse muutmise seaduse eelnõu juurde. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/b1803bfa-8bbb-b0cb-8963-5ce82b555dc7/Elektroonilise%20side%20seaduse%20ja%20info%C3%BChiskonna%20teenuse%20seaduse%20muutmise%20seadus, 01.04.2018.
30. Seletuskiri isikuandmete kaitse seaduse eelnõu juurde. 1995. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/d96af9b4-d9f7-3c77-b6d1-9808941749d2/Isikuandmete%20kaitse%20seadus, 01.04.2018.
31. Seletuskiri kindlustustegevuse seaduse, finantsinspektsiooni seaduse ja isikuandmete kaitse seaduse muutmise seaduse eelnõu juurde. Kättesaadav: https://www.riigikogu.ee/download/60592fe9-506e-e74d-0e1d-33cb5384a1fa, 01.04.2018.
32. The European Commission. DG Justice, Freedom and Security. Study on the economic benefits of privacy enhancing technologies. London Economics: 2010. Available: https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf, 01.04.2018.
33. Tupay, P. K. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigusisikuandmete kaitsele. - Juridica 2016, IV.
34. Varul, P. ja teised. Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne. Tallinn, 2010.
35. Westin, A.F. Privacy and Freedom. 25 Washington & Lee Law Review 166. New York: Athenum 1968. Available: https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr, 02.04.2018.

Kasutatud õigusaktid

36. Advokatuuriseadus. - RT I 2001, 36, 201... RT I, 20.04.2017, 4.
37. Eesti Vabariigi põhiseadus. - RT 1992, 26, 349... RT I, 27.04.2011, 2.
38. Elektroonilise side seadus. - RT I 2004, 87, 593... RT I, 01.07.2017, 2.
39. Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja Nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). 10.1.2017.

40. Euroopa inimõiguste ja põhivabaduste konventsioon. - RT II 1996, 11, 34. Vastu võetud 4.11.1050, Eestis jõustunud 16.04.1996.
41. Euroopa Liidu põhiõiguste harta. - ELT C 83, 30.03.2010.
42. Euroopa Parlamendi ja nõukogu 24.10.1995 direktiiv üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. - ELT L 281, 23.11.1995.
43. Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris. ELT L 201, 31.07.2002. (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (viimane konsolideeritud versioon).
44. Infoühiskonna teenuse seadus. - RT I 2004, 29, 191... RT I, 12.07.2014, 48.
45. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. (jõustunud 28.01.1981). - RT II 2001, 1.
46. Isikuandmete kaitse seadus. - RT I 1996, 48, 944.
47. Isikuandmete kaitse seadus. - RT 2003, 26, 158.
48. Isikuandmete kaitse seadus - RT I 2007, 24, 127… RT I, 06.01.2016, 10.
49. Isikuandmete kaitse seadus. Eelnõu 21.03.2018. Kättesaadav: http://eelnoud.valitsus.ee/main#JoVLoWNP, 01.04.2018.
50. Isikuandmete kaitse seaduse rakendamise seadus. Eelnõu 23.03.2018. Kättesaadav: http://eelnoud.valitsus.ee/main#Fkf86wSO, 01.04.2018.
51. Kindlustustegevuse seadus. - RT I, 07.07.2015, 1...RT I, 17.11.2017, 49
52. Krediidiasutuste seadus. - RT I 1999, 23, 349... RT I, 30.12.2017, 31
53. Rahapesu ja terrorosmi tõkestamise seadus. - RT I, 17.11.2017.
54. ÜRO inimõiguste ülddeklaratsioon A/RES/217, 10.12.1948.

Kasutatud kohtupraktika

55. EIKo 20.06.2017, 13812/09, *Bogomolova* vs. *Russia*.
56. EKo 02.12.2010, C-108/09, *Ker-Optika*.
57. EKo 16.10.2012, C-614/10, *Commission* vs *Austria*.
58. EKo 05.05.2011, C-53/09, *Deutsche Telekom AG* vs. *Saksamaa*.
59. EKo 09.11.2010, C-92/09 ja C-93/09, *Volker und Markus Schecke* vs. *Land Hessen*.
60. RKHK 12.06.2012, 3-3-1-3-12.
61. RKHK 12.12.2011, 3-3-1-70-11.
62. RKTK 18.02.2015, 3-2-1-159-14.
63. RKTK 29.03.2017, 3-2-1-153-16.

Muud allikad

64. A comprehensive approach on personal data protection in the European Union. Communication from the commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. Brussels, 4.11.2010 COM (2010) 609 final. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0609, 01.04.2018.
65. Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Personal data used for the purposes of direct marketing. Available: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=605791&SecMode=1&DocId=688244&Usage=2, 01.04.2018.
66. Andmekaitse Inspektsioon. Elektrooniliste kontaktandmete kasutamine otseturustuseks. Kättesaadav: http://www.aki.ee/et/juhised, 01.04.2018.
67. Andmekaitse Inspektsioon. Informeeritud nõusolek isikuandmete töötlemiseks. 01.03.2013. Kättesaadav: http://www.aki.ee/et/mida-peab-teadma-isikuandmete-tootlemisest/informeeritud-nousolek-isikuandmete-tootlemiseks, 02.04.2018.
68. Andmekaitse Inspektsioon. Andmekaitse Inspektsiooni peadirektori ülevaade ELi andmekaitsereformi rakendamise seisust Eestis. 14.10.2016. Kättesaadav: http://www.aki.ee/et/eraelu-kaitse/euroopa-andmekaitse-reform, 02.04.2018.
69. Appendix to Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical data. Available: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=564487&SecMode=1&DocId=560582&Usage=2, 01.04.2018.
70. Article 29 Data Protection Working Party. Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). WP 128. Brussels: 2006. Available: http://www.dataprotection.ro/servlet/ViewDocument?id=234, 01.04.2018.
71. Article 29 Data Protection Working Party. Guidelines on Article 49 of Regulation 2016/679. WP 262. Brussels: 2018. Available: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614232, 01.04.2018.
72. Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. WP 251. Brussels: 2017. Available: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, 01.04.2018.

73. Article 29 Data Protection Working Party. Guidelines on Consent Under Regulation 2016/679. WP 259. Brussels: 2017. Adopted on 28.11.2017. Available: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239, 01.04.2018.
74. Article 29 Data Protection Working Party. Guidelines on Transparency Under Regulation 2016/679. WP 260. Brussels: 2017. Available: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615250, 01.04.2018.
75. Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent. WP 187. Brussels: 2011. Available: http://ec.europa.eu/newsroom/article29/news-overview.cfm, 01.04.2018.
76. Article 29 Data Protection Working Party. Opinion 2/2010 on behavioral advertising. WP 171. Brussels: 2010. Available: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/junio/WP171en.pdf, 1.04.2018.
77. Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. WP 203. Brussels: 2013. Available: https://cnpd.public.lu/content/dam/cnpd/fr/publications/groupe-art29/wp203_en.pdf, 01.04.2018.
78. Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. WP 217. Brussels: 2014. Available: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2014/04/wp217_en.pdf, 01.04.2018.
79. Centre for Information Policy Leadership. Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Consent", adopted on 28 November 2017. Available: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_guidelines_on_consent-c.pdf, 01.04.2018.
80. E-Privacy Regulation will not come into force until 2019. - Press release. 24.11.2017. Available: https://www.eprivacy.eu/en/about-us/news-press/news-detail/article/eprivacy-regulation-will-not-come-into-force-until-2019/, 01.04.2018.
81. Euroopa Komisjon. Kes on vastutav töötleja või volitatud töötleja? Kättesaadav: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and organisations/obligations/controller-processor/what-data-controller-or-data-processor_et, 01.04.2018.
82. Andmekaitse Inspektsioon. Pankade seire seoses isikuandmete töötlemisega nõusoleku alusel ja lepingu täitmiseks. Isikuandmete kaitse seaduse täitmise seire. Tallinn: 2013. Kättesaadav:

http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Pankade_seire2013.pdf, 01.04.2018.

83. Opinion of Advocate General Sharpston delivered on 17 June 2010, Volker und Markus Schecke GbR, in Joined Cases C-92/09 and C-93/09. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CC0092, 02.04.2018.
84. The Economist. The world's most valuable resource. London: 06.05.2017. https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource, 01.04.2018.
85. The Information Commissioner. Monetary penalty notice to Honda Motor Europe Limited t/a Honda (U.K.). London: 20.03.2017. Available: https://ico.org.uk/media/action-weve-taken/mpns/2013732/mpn-honda-europe-20170320.pdf, 01.04.2018.
86. The Information Commissioner. Monetary penalty notice to Moneysupermarket.com Ltd. London: 17.07.2017. Available: https://ico.org.uk/media/action-weve-taken/mpns/2014482/mpn-moneysupermarket-ltd-20170720.pdf, 01.04.2018.
87. Õiguskantsleri märgukiri e-postile edastatava reklaami kohta. 05.2008. Kättesaadav: http://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_margukiri_e-posti_aadressile_edastatav_reklaam.pdf, 01.04.2018.
88. Õiguskantsleri märgukiri KindlTS § 14^2 lg 2 ja KAS § 89 lg 2^2 ja 2^3 põhiseaduspärasuse kohta. 26.02.2014. Kättesaadav: http://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_oigus_votta_nousolek_isikuandmete_tootlemiseks_tuuptingimustes.pdf, 01.04.2018.
89. Euroopa Komisjon. Komisjoni teatis Euroopa parlamendile, nõukogule, majandus- ja sotsiaalkomiteele ning regioonide komiteele. Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus, KOM(2010) 609 lõplik. Brüssel: 04.11.2010. Kättesaadav: https://ec.europa.eu/health//sites/health/files/data_collection/docs/com_2010_0609_et.pdf, 01.04.2018.
90. Stadnik, A. Andmekaitseseadusega kaasnevad suured trahvid on müüt. 10.11.2016. Kättesaadav: https://www.aripaev.ee/uudised/2016/11/10/andmekaitseseadusega-kaasnevad-suured-trahvid-on-muut, 01.04.2018.
91. Peep, V. Kas isikuandmete kaitse üldmäärus toob tõesti kaasa hiigeltrahvid? 15.11.2017. Kättesaadav: http://www.aki.ee/et/uudised/uudiste-arhiiv/kas-isikuandmete-kaitse-uldmaarus-toob-toesti-kaasa-hiigeltrahvid, 01.04.2018.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Sandra Velbri

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Isikuandmete kaitse üldmäärusest tulenev nõusoleku vajadus ja selle tingimused isikuandmete töötlemisel äriühingute poolt", mille juhendaja on Sandra Sillaots ja kaasjuhendaja Ülle madise

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