TARTU ÜLIKOOL

SOTSIAALTEADUSTE VALDKOND

ÕIGUSTEADUSKOND

Avaliku õiguse osakond

Kristena Paalmäe

ANDMETE ÜLEKANDMISE ÕIGUS ISIKUANDMETE KAITSE ÜLDMÄÄRUSES

Magistritöö

Juhendaja: *dr. iur*. Mario Rosentau

Kaasjuhendaja: *mag. iur.* Annika Vait

Tartu

2019

SISUKORD

SISSEJUHATUS

Andmete kogumine, töötlemine, vahetamine ja kasutamine on tehnoloogilise arengu ja üleilmastumise[1] tõttu võtnud tänapäevases maailmas täiesti uue mõõtme. Aina uute tehnoloogiliste lahenduste kasutuselevõtmine võimaldab andmete lihtsat ja vaba liikumist üle kogu maailma. Sealjuures ei tohiks jätta tähelepanuta, kuidas kaitstakse andmeid ja andmesubjektide õigusi.

2018. aastal tugevalt päevakorda tõusnud Euroopa andmekaitsevaldkonnas võeti vastu uus regulatsioon: alates 25.05.2018. a hakkas kehtima Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).[2] Avalikkuse tähelepanu pälvinud isikuandmete kaitse üldmäärusest (ingliskeelse lühendina tuntud kui *GDPR – General Data Protection Regulation*, käesolevas töös edaspidi nimetatud kui üldmäärus) on palju räägitud nii praktilisel kui ka õigusteaduslikul tasandil.[3] Andmekaitsevaldkonna tõusmine avalikkuse tähelepanu alla on vägagi tervitatav, sest aitab laiemalt teadvustada isikuandmete kaitset kui põhiõigust ning selle kaitsmise vajalikkust maailmas, kus infovoog aina suureneb.

Üldmäärus asendab Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta[4]. Nimetatud direktiivi osas on erialakirjanduses väljendatud arvamust, et see ei suutnud täita oma eesmärke ega EL-s andmekaitse taset ühtlustada, sest EL liikmesriikide poolt vastu võetud erinevate õigusaktide tõttu olid andmekaitsevaldkonnas liikmesriigiti olulised õiguslikud erinevused: ühes liikmesriigis lubatud andmetöötlus võis olla teises liikmesriigis õigusvastane.[5] Andmekaitse killustatust EL liikmesriikide seas ja sellest tulenevat õiguslikku ebakindlust peeti majandustegevust moonutavaks konkurentsiks ja takistuseks ametiasutustele nende liidu õigusest tulenevate kohustuste täitmisel.[6]

---

[1] D. Rücker. Development and Importance of the Data Protection Reform. – New European General Data Portection Regulation: A Practitioner's Guide. Nomos Verlagsgesellschaft, Baden-Baden 2018, lk 1.
[2] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119/1, 04.05.2016, lk 1–88.
[3] Mahukamatest käsitlustest vt nt P. Voigt, A. von dem Bussche 2017, P. B. Lambert 2018.
[4] Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EÜT L 281, 23.11.1995, lk 31-50.
[5] P. Voigt, A. von dem Bussche. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing AG 2017, lk 2.
[6] Üldmäärus, põhjenduspunkt 9.

Võrreldes varem kehtinud direktiiviga, on 25.05.2018. a jõustunud üldmäärus tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.[7] Üldmääruse vahetu kohaldatavus aitab tagada füüsiliste isikute järjekindlat ja kõrgetasemelist kaitset ning kõrvaldada takistusi isikuandmete liikumisel liidus ning füüsiliste isikute õiguste ja vabaduste kaitse peaks andmete töötlemisel olema kõigis liikmesriikides samal tasemel.[8] Siiski on juba väljendatud ka teistsugust arvamust: kuivõrd üldmäärus sisaldab üle 50 paindlikkusklausli[9], jätab see liikmesriikidele laia otsustusruumi, mis ei aita saavutada ühetaolise andmekaitse eesmärki.[10]

Euroopa Liidus tunnustatakse õigust isikuandmete kaitsele põhiõigusena. Üldmääruse artiklis 1 on sätestatud, et füüsiliste isikute kaitse isikuandmete töötlemisel on põhiõigus. Euroopa Liidu põhiõiguste harta[11] (edaspidi nimetatud kui harta) artikli 8 lõikes 1 ja Euroopa Liidu toimimise lepingu (edaspidi nimetatud kui ELTL) artikli 16 lõikes 1 on sätestatud, et igaühel on õigus oma isikuandmete kaitsele. Inimõiguste ja põhivabaduste kaitse konventsiooni[12] (edaspidi nimetatud kui EIÕK) artikkel 8 sätestab samuti õiguse austusele era- ja perekonnaelu vastu. Euroopa Kohus on väljendanud seisukohta *Volker und Markus Schecke* kohtuasjas, et õigus isikuandmete kaitsele ei ole absoluutne õigus, vaid sellega tuleb arvestada vastavalt selle ülesandele ühiskonnas.[13]

Üheks üldmääruse eesmärgiks on anda andmesubjektidele suurem kontroll nende isikuandmete üle.[14] Kontrolli teostamiseks on andmesubjektidel võimalik kasutada üldmäärusest tulenevaid andmesubjekti õigusi, kuid seda saab teha üksnes juhul, kui andmesubjekt on üleüldse teadlik sellest, et tema isikuandmeid töödeldakse.[15] Eelkõige kontrolli andmise eesmärgil on üldmäärusega mitmete teiste muudatuste kõrval kehtestatud täiesti uue andmesubjekti õigus, milleks on õigus andmete ülekandmisele. Käesoleva magistritöö uurimisobjektiks olev õigus andmete ülekandmisele on sätestatud üldmääruse artiklis 20. Lühidalt on selle sisuks andmesubjekti õigus saada kas vastutavalt töötlejalt koopia isikuandmetest, mida vastutav töötleja tema kohta hoiab, kanda andmed ise teise vastutava töötleja juurde üle või nõuda

[7] A. D. Vanberg, M. B. Ünver. The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? – European Journal of Law and Technology, 2017/8, No 1, lk 2.
[8] Üldmäärus, põhjenduspunkt 10.
[9] Paindlikkusklauslid on vahetult kohaldatava määruse erandid, mis võimaldavad liikmesriikidel asjaomastes küsimustes iseseisvaid riiklikke norme kehtestada. – P. K. Tupay. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. – Juridica 2016/IV, lk 238, viide 130.
[10] P. K. Tupay, lk 238-239 (viidatud: Saksamaa Liitvabariigi andmekaitse ja informatsioonivabaduse inspektroni Andrea Voßhoffi seisukoht, lk 1 jj; Austria andmekaitseeksperdi Waltraud Kotschy arvamus; Kasseli Ülikooli professori Alexander Roßnageli seisukoht).
[11] Euroopa Liidu põhiõiguste harta. – ELT 2012/C 326/02.
[12] Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II, 2000, 11, 57.
[13] EKo C-92/09, *Volker und Markus Schecke*, p 48 (viidatud: EKo 112/00, *Schmidberger*, p 80 ja seal viidatud kohtupraktika).
[14] Üldmäärus, põhjenduspunkt 7.
[15] P. Voigt, A. von dem Bussche, lk 147.

vastutavalt töötlejalt andmete otse ülekandmist teise vastutava töötleja juurde, kui see on tehniliselt teostatav.

Andmete ülekandmise õigus on väga aktuaalne uurimisprobleem, sest see on nii andmekaitsevaldkonnas kui ka laiemalt täiesti uudne õigus. Varasemalt on andmete ülekandmise õigusega sarnanevaid õigusi autorile teadaolevalt kehtestatud üksnes telekommunikatsiooni valdkonnas: näiteks universaalteenuste direktiiviga on kehtestatud telefoninumbrite teisaldamise õigus[16] ning raamdirektiiv elektrooniliste sidevõrkude ja –teenuste ühise reguleeriva raamistiku kohta toetab interaktiivse sisu teisaldamist edastusmehhanismide vahel.[17] Teiseks kinnitab teema aktuaalsust ka eestikeelse kirjanduse ja (õigus)praktika vähesus. Samal ajal on ingliskeelses õiguskirjanduses on juba mitmel korral andmete ülekandmise õigusega seonduvatele probleemkohtadele tähelepanu juhitud või neid analüüsitud, kuid mitte ammendavalt. Kolmandaks muudab töö eriti oluliseks ja aktuaalseks see, et autorile teadaolevalt ei ole varasemalt üldse käsitletud seda, kuidas andmete ülekandmise õigus mõjutab kolmandate isikute õigusi kui andmete ülekandmise käigus kantakse ühe vastutava töötleja juurest teise juurde üle ka kolmanda isiku isikuandmed. Seetõttu peab autor käesoleva magistritöö teemat andmekaitsevaldkonnas aktuaalseks ja oluliseks.

Käesolevas magistritöös uuritakse andmete ülekandmise õiguse sisu, rakendamise eelduseid, eesmärke ja seost teiste andmesubjekti õigustega. Samuti on fookuses nii andmeid saatva kui andmeid vastuvõtva vastutava töötleja kohustused andmete ülekandmisel ja isikuandmete turvalisus andmete ülekandmisel. Töös on välja toodud, et võib esineda olukordi, kus andmete ülekandmise õiguse teostamisel kantakse ühes andmesubjekti isikuandmetega uue vastutava töötleja juurde üle ka kolmandat isikut puudutavad isikuandmed. Seetõttu on magistritöö eesmärk analüüsida kolmandate isikute õigust eraelu puutumatuse ja isikuandmete kaitsele juhul, kui andmete ülekandmise õiguse teostamisel kantakse ühes andmesubjekti andmetega uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmeid. Ühtlasi on töö fookuses see, kuidas kaitstakse ülekantud andmeid uue vastutava töötleja juures.

[16] Euroopa Parlamendi ja nõukogu direktiiv 2002/22/EÜ, 7. märts 2002, universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul (universaalteenuse direktiiv), artikkel 30. – EÜT L 108, 24.4.2002, lk 51—77 (eestikeelne eriväljaanne: ptk 13, kd 029, lk 367 – 393).

[17] Euroopa Parlamendi ja nõukogu direktiiv 2002/21/EÜ, 7. märts 2002, elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv), põhjenduspunkt 31. – EÜT L 108, 24.4.2002, lk 33—50 (eestikeelne eriväljaanne: ptk 13, kd 029, lk 349 – 366).

Magistritöö otsib kinnitust kolmele hüpoteesile:

1. Andmete ülekandmise õiguse teostamine riivab kolmandate isikute eraelu puutumatuse ja isikuandmete kaitse õigust, kui andmete ülekandmise õiguse teostamisel kantakse uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed;
2. Vastutaval töötlejal ei ole võimalik keelduda kolmanda isiku õiguste ja vabaduste kaitse põhjendusel andmesubjekti esitatud andmete ülekandmise taotluse täitmisest;
3. Kui andmete ülekandmise õiguse teostamisel kantakse uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed, kaotab kolmas isik oma isikuandmete üle kontrolli ega saa kasutada üldmäärusest tulenevaid andmesubjekti õigusi, välja arvatud juhul, kui uus vastutav töötleja määrab kolmanda isiku isikuandmete töötlemisele õigusliku aluse ja teavitab sellest uut andmesubjekti.

Esimeses peatükis annan ülevaate andmete ülekandmise õiguse teostamisest ja analüüsin, millised on õiguslikud alused andmete ülekandmise õiguse tekkimiseks. Samuti analüüsin, millistel eeldustel saab andmesubjekt nõuda andmete ülekandmist vastutavalt töötlejalt ning kuidas nimetatud eelduseid sisustada. Esimeses peatükis käsitlen ka seda, millised on andmeid saatva ja andmeid vastuvõtva vastutava töötleja õigused ja kohustused andmete ülekandmise õiguse korral. Samuti uurin, millised on andmesubjekti võimalikud turvariskid andmete ülekandmise õiguse teostamisel ja kuidas neid vältida.

Teises peatükis analüüsin, kas leiab kinnitust magistritöö esimene hüpotees, et andmete ülekandmise õiguse teostamine riivab kolmandate isikute eraelu puutumatuse ja isikuandmete kaitse õigust, kui andmete ülekandmise õiguse teostamisel kantakse uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed. Väljakujunenud Euroopa Kohtu praktikast tulenevalt ei ole põhiõigused absoluutsed õigused, vaid neile võib seada piiranguid tingimusel, et need piirangud vastavad tegelikult meetmega taotletud üldise huvi eesmärkidele ega kujuta endast taotletavat eesmärki arvestades ülemäärast ja lubamatut sekkumist, mis kahjustaks tagatud õiguste sisu.[18] Kolmandate isikute õiguste võimaliku riive hindamisel tuleb neid aspekte hinnata. Analüüsimisel võtan aluseks Euroopa Kohtu praktikas väljakujunenud kriteeriumid: kas piirang on seadusega ette nähtud, kas piirang järgib ühte või mitut legitiimset eesmärki ja kas piirang on selle eesmärgi või nende eesmärkide saavutamiseks demokraatlikus ühiskonnas vajalik?[19]

[18] EKo C-418/11, *Texdata Software*, p 84 (viidatud: EKo C-28/05, *Dokter*, p 75 ja ühendatud kohtuasjad EKo C-317/08 ja C-320/08, *Alassini* p 63).
[19] EKo liidetud kohtuasjades C-465/00, C-138/01 ja C-139/01, *Österreichischer Rundfunk.*

Kolmandas peatükis analüüsin, kuidas on üldmääruses tagatud kolmandate isikute õiguste ja vabaduste kaitse andmete ülekandmise õiguse teostamise korral. Selleks tuvastan, kas vastutav töötleja saab kolmandate isikute õiguste ja vabaduste kaitseks andmete ülekandmise taotluse täitmisest keelduda. Seeläbi annan hinnangu, kas leiab kinnitust magistritöö teine hüpotees, et vastutaval töötlejal ei ole võimalik keelduda kolmandate isikute õiguste ja vabaduste kaitse põhjendusel andmesubjekti esitatud andmete ülekandmise taotluse täitmisest. Kolmandate isikute õiguste kaitsega seonduvalt otsin kinnitust ka kolmandale hüpoteesile: kui andmete ülekandmise õiguse teostamisel kantakse üle ka kolmanda isiku isikuandmed uue vastutava töötleja juurde, kaotab kolmas isik oma isikuandmete üle kontrolli ega saa kasutada üldmäärusest tulenevaid andmesubjekti õigusi.

Käesoleva magistritöö eesmärkide saavutamiseks kasutan kombineeritud meetodina sünteetilist, analüütilist ja süsteemset meetodit. Sünteetilise meetodi (käsitlus üksikult üldisele) valimise põhjuseks on allikmaterjalidena kasutatavast kohtupraktikast üldistavate järelduste tegemine. Analüütilist meetodit (käsitlus üldiselt üksikule) on asjakohane kasutada läbivalt. Süsteemset meetodit (probleemide kompleksne, seostatud käsitlus) kasutan seetõttu, et üldmääruse regulatsiooni mahukust ja olemust arvestades on asjakohane esitatud hüpoteesidele kinnitust otsides tugineda üldmääruse erinevatele sätetele erinevatest peatükkidest.

Peamiselt tugineb töö võõrkeelsele õiguskirjandusele, sest magistritöö kirjutamise ajal on kõnealusel teemal eestikeelset õiguskirjandust veel vähe. Lisaks sellele on allikatena kasutatud Eesti ja EL õigusakte, õigusaktide kommentaare, Euroopa Andmekaitsenõukogu ja artikli 29 alusel asutatud andmekaitse töörühma suuniseid, samuti Riigikohtu, Euroopa Kohtu ja Euroopa Inimõiguste Kohtu lahendeid.

Märksõnad: andmekaitse, andmetöötlus, isikuandmed, eraelu, põhiõigused.

1. ANDMETE ÜLEKANDMISE ÕIGUS

1.1.Andmete ülekandmise õiguse olemus ja sisu

Andmete ülekandmise õigus on üldmäärusega kehtestatud täiesti uus andmesubjekti õigus. Isikuandmete kaitse üldmääruse eelkäija, direktiiv 95/46/EÜ, sellist õigust andmesubjektile ette ei näinud.[20] Andmete ülekandmise õiguse sätestab üldmääruse artikkel 20, mille edaspidise käsitluse paremaks mõistmiseks on järgnevalt tsiteeritud kogu säte:

1. Andmesubjektil on õigus saada teda puudutavaid isikuandmeid, mida ta on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul ning õigus edastada need andmed teisele vastutavale töötlejale, ilma et vastutav töötleja, kellele kõnealused isikuandmed on esitatud, seda takistaks, kui

a) töötlemine põhineb artikli 6 lõike 1 punktis a või artikli 9 lõike 2 punktis a osutatud nõusolekul või artikli 6 lõike 1 punktis b osutatud lepingul ning

b) töödeldakse automatiseeritult.

2. Kui andmesubjekt kasutab lõike 1 kohaselt andmete ülekandmise õigust, on tal õigus nõuda, et vastutav töötleja edastab andmed otse teisele vastutavale töötlejale, kui see on tehniliselt teostatav.

3. Käesoleva artikli lõikes 1 nimetatud õiguse kasutamine ei piira artikli 17 kohaldamist. Seda õigust ei kohaldata töötlemise suhtes, mis on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks.

4. Lõikes 1 osutatud õigus ei kahjusta teiste isikute õigusi ja vabadusi.

Sisuliselt tähendab andmete ülekandmise õigus andmesubjekti õigust saada vastutava töötleja käest koopia andmesubjekti puudutavatest isikuandmetest ning viia isikuandmed üle teise vastutava töötleja juurde.[21] Seega koosnebki õigus andmete ülekandmisele kolmest elemendist: esiteks on andmesubjektil õigus saada vastutavalt töötlejalt koopia isikuandmetest, mida vastutav töötleja tema kohta hoiab (artikkel 20 lg 1), teiseks, on andmesubjektil õigus saadud andmed ise teise vastutava töötleja juurde üle kanda (artikkel 20 lg 1), ning kolmandaks, on

[20] J. Schrey. General conditions for data processing in companies under the GDPR. – D. Rücker, T. Kugler. New European General Data Protection Regulation: A Practitioner's Guide. Nomos Verlagsgesellschaft, Baden-Baden 2018, lk 144.
[21] D. Kelleher, K. Murray. EU Data Protection Law. Bloomsbury Professional 2018, lk 217.

andmesubjektil õigus nõuda andmete otse ülekandmist ühe vastutava töötleja juurest teise juurde, kui see on tehniliselt teostatav (artikkel 20 lg 2).[22]

Samas on ka erialakirjanduses peetud piisavaks üksnes kahe andmete ülekandmise õiguse põhielemendi eristamist: esiteks, andmesubjektil on õigus saada vastutavalt töötlejalt koopia andmesubjekti puudutavatest isikuandmetest, ja teiseks, andmesubjektil on õigus kanda andmed üle ühe vastutava töötleja juurest teise juurde.[23] Üldmääruse artikli 20 lg-te 1 ja 2 sõnastust täpselt järgides ei ole selline arusaam siiski piisavalt täpne. Üldmääruse artikli 20 lg 1 sõnastusest nähtub, et andmesubjektil on õigus saada teda puudutavaid isikuandmeid ja õigus edastada need andmed teisele vastutavale töötlejale. Artikli 20 lg-s 1 kasutatav sõnastus viitab andmete ülekandmise õiguse teostamisel andmesubjekti enda aktiivsele tegevusele, millega andmesubjekt kas soovib saada endale koopia teda puudutavatest isikuandmetest või edastada need ise teisele vastutavale töötlejale. Artikkel 20 lg-st 1 tulenevad seega kaks eraldiseisvat andmete ülekandmise õiguse elementi. Lisaks saab artikli 20 lg 2 järgi andmesubjekt lõikes 1 nimetatud õigust kasutades nõuda, et vastutav töötleja edastab andmed otse teisele vastutavale töötlejale. Artikli 20 lg 2 sõnastusest nähtuvalt on tegemist eraldi andmete ülekandmise õiguse elemendiga, sest artikli 20 lg-s 2 sisalduva õiguse rakendamisel on vajalik vastutava töötleja tegevus, mitte enam andmesubjekti tegevus. Seega nõustub autor ülaltoodud seisukohaga,[24] et andmete ülekandmise õigus kätkeb endas kolme eraldi elementi (andmesubjekti õigust).

Õigust andmete ülekandmisele saab käsitleda kui edasiarendust andmesubjekti õigusest tutvuda andmetega, mille sätestab üldmääruse artikkel 15.[25] Võrreldes andmetega tutvumise õigust ja andmete ülekandmise õigust, võimaldab andmetega tutvumise õigus andmesubjektil tutvuda mitte üksnes andmetega, mille andmesubjekt on ise vastutavale töötlejale esitanud, vaid üldmääruse artikkel 15 lg 1 sätestab laiema loetelu andmetest, millega andmesubjekt tutvuda saab. Seega andmetega tutvumise õiguse kohaldamisala on hõlmatud isikuandmete aspektist vaadatuna laiem kui andmete ülekandmise õiguse puhul. Lisaks vastutavalt töötlejalt teabe saamisele võimaldab õigus andmete ülekandmisele andmesubjekti efektiivsemat kontrollifunktsiooni teda puudutavate isikuandmete üle, sest lubab andmed teise vastutava töötleja juurde üle kanda.[26] Siiski saab andmesubjekt isikuandmed teise vastutava töötleja

[22] P. de Hert jt. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. – Computer Law & Security Review 2018/34, Issue 2, lk 197.
[23] A. D. Vanberg, M. B. Ünver, lk 2.
[24] Vt viide 22.
[25] A. D. Vanberg, M. B. Ünver, lk 2.
[26] P. de Hert jt, lk 201.

juurde üle kanda üksnes ulatuses, milles andmesubjekt on ise vastutavale töötlejale teda puudutavad andmed esitanud.

1.2.Andmete ülekandmise õiguse seos andmesubjekti muude õigustega

Kuivõrd andmete ülekandmise õigus on üks mitmest üldmääruses sisalduvast andmesubjekti õigusest, siis tuleb määratleda, milline on andmete ülekandmise õiguse seos teiste andmesubjekti õigustega.

Andmesubjekti õigused sisalduvad üldmääruse artiklites 15-22, mille järgi on andmesubjektil õigus tutvuda andmetega (üldmääruse artikkel 15), õigus andmete parandamisele (üldmääruse artikkel 16), õigus andmete kustutamisele („õigus olla unustatud“, üldmääruse artikkel 17), õigus isikuandmete töötlemise piiramisele (üldmääruse artikkel 18), õigus tagada kolmandate isikute teavitamine isikuandmete parandamisest või kustutamisest (üldmääruse artikkel 19), õigus andmete ülekandmisele (üldmääruse artikkel 20), õigus esitada vastuväiteid (üldmääruse artikkel 21) ja õigus mitte olla automatiseeritud töötlemisel põhinevate üksikotsuste tegemise, sh profiilianalüüsi subjektiks (üldmääruse artikkel 22).

Andmete ülekandmise taotluse esitamine vastutavale töötlejale ei piira andmesubjekti õigust kasutada muid üldmäärusest tulenevaid andmesubjekti õigusi.[27] Selline põhimõte kehtib kõikide üldmääruses sisalduvate õiguste puhul.[28] Seega, kui andmesubjekt on esitanud vastutavale töötlejale andmete ülekandmise taotluse, võib andmesubjekt vastutavale töötlejale esitada ka teisi taotlusi.

Eraldi sätestab üldmääruse artikkel 20 lg 3, et käesoleva artikli lõikes 1 nimetatud andmete ülekandmise õiguse kasutamine ei piira artikli 17 kohaldamist (s.o andmete kustutamise õiguse kasutamist). See tähendab, et kui andmesubjekt on esitanud vastutavale töötlejale taotluse andmete ülekandmiseks, ei kaasne sellega vastutava töötleja kohustust ülekantud andmed kustutada. Seega ei too andmesubjekti jaoks andmete ülekandmise õiguse kasutamine kaasa ülekantud andmete kustutamist vastutava töötleja juures.[29]

1.3.Andmete ülekandmise õiguse eesmärk

Andmete ülekandmise õiguse kehtestamise eesmärgid on vaadeldavad nii majanduslike kui andmekaitseliste eesmärkidena.

---

[27] Artikli 29 alusel asutatud andmekaitse töörühm. Suunised andmete ülekandmise õiguse kohta, kinnitatud Euroopa Andmekaitsenõukogu poolt 05.04.2017. Kättesaadav veebis: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233, lk 7.
[28] Artikli 29 töörühm, lk 7.
[29] Artikli 29 töörühm, lk 7.

Andmete ülekandmise õiguse esimeseks ja põhiliseks eesmärgiks on tugevdada andmesubjekti kontrolli teda puudutavate isikuandmete üle ja veenduda, et andmesubjektidel on andmete ökosüsteemis aktiivne roll.[30] See on andmekaitseline eesmärk. Võimalus oma isikuandmeid kergesti ühe vastutava töötleja juurest teise juurde liigutada, kopeerida või üle kanda annab andmesubjektile suurema kontrolli teda puudutavate isikuandmete üle. Seeläbi andmesubjektile antav kontroll oma isikuandmete üle suurendab tema usaldust kogu internetikeskkonda,[31] mille vahendusel toimub suurem osa tänapäevasest andmevahetusest. Ühtlasi aitab andmesubjektile teda puudutavate andmete üle suurema kontrolli andmine tasakaalustada andmesubjekti ja vastutavate töötlejate vahelist suhet.[32]

Teine eesmärk on vältida andmesubjekti „kinnijäämist" ühe teenusepakkuja (vastutava töötleja) juurde.[33] Kinnijäämine ühe teenusepakkuja juurde tekib põhjusel, et esimestel teenusepakkujatel, kelle juures andmesubjekt registreerub või kelle teenuseid kasutama asub, on võimalus koguda isikute kohta rohkelt isikuandmeid ja seeläbi võivad nad kehtestada teistele teenusepakkujatele takistusi turule sisenemiseks. Ühtlasi saavad nn esimesed teenusepakkujad muuta andmesubjekti jaoks teenusepakkuja vahetamise liialt kulukaks või koormavaks.[34] Andmesubjekti kinnijäämise vältimise eesmärk on käsitletav pigem majandusliku eesmärgina.

Ka kolmas eesmärk on käsitletav majandusliku eesmärgina ning on tihedalt seotud konkurentsiõigusega. Andmete ülekandmise õiguse kolmas eesmärk on saavutada EL ühisturul suurem konkurents vastutavate töötlejate vahel,[35] tagades andmesubjektidele õiguse neid puudutavate isikuandmete ülekandmiseks ühe vastutava töötleja juurest teise juurde. Direktiivi 95/46/EÜ artikli 29 alusel asutatud andmekaitse töörühm (edaspidi: artikli 29 töörühm) on avaldanud suunised andmete ülekandmise õiguse kohta. Kuigi artikli 29 alusel asutatud andmekaitse töörühm on käesolevaks ajaks tegevuse lõpetanud, loodi selle asemel üldmääruse artikkel 68 alusel Euroopa Andmekaitsenõukogu (ingl k *European Data Protection Board*). Euroopa Andmekaitsenõukogu on 05.04.2017. a seisuga üle vaadanud ja kinnitanud artikli 29 töörühma antud suunised andmete ülekandmise õiguse kohta. Artikli 29 töörühm selgitab, et „kuna andmete ülekandmise õigus võimaldab edastada isikuandmeid otse ühelt vastutavalt töötlejalt teisele, on see ka oluline vahend, mis toetab isikuandmete vaba liikumist ELis ja soodustab vastutavate töötlejate vahelist konkurentsi."[36] Andmete ülekandmise õiguse

[30] Artikli 29 töörühm, lk 4.
[31] B. Van der Auwermeulen, lk 68.
[32] Artikli 29 töörühm, lk 4.
[33] J. Schrey, lk 144.
[34] B. Van den Auwermeulen, lk 58.
[35] D. Kelleher, K. Murray, lk 217.
[36] Artikli 29 töörühm, lk 3.

konkurentsi soodustav olemus väljendub selles, et kui vastutavad töötlejad võimaldavad andmete ülekandmist ega keeldu sellest alusetult, aitab see vähendada turgu valitseva positsiooni omamist ja parandada konkurentsi vastutavate töötlejate vahel.[37]

1.4.Eeldused andmete ülekandmise õiguse teostamiseks

1.4.1. Andmesubjekti nõusolek ja leping

Üldmääruse artikkel 20 lg 1 p a sätestab, et andmesubjektil on õigus saada teda puudutavaid isikuandmeid ning õigus edastada need andmed teisele vastutavale töötlejale, kui töötlemine põhineb artikli 6 lõike 1 punktis a või artikli 9 lõike 2 punktis a osutatud nõusolekul või artikli 6 lõike 1 punktis b osutatud lepingul. See tähendab, et andmete ülekandmise õiguslikuks aluseks saab olla üksnes andmesubjekti nõusolek või andmesubjekti osalusel sõlmitud leping.

Isikuandmete töötlemine andmesubjekti nõusolekul saab põhineda kas üldmääruse artikli 6 lg 1 punktil a, või kui tegemist on isikuandmete eriliikide töötlemisega, üldmääruse artikli 9 lg 2 punktil b. Mõlemal juhul peab andmesubjekti nõusolek vastama üldmääruse artikli 7 lg-st 2 tulenevatele tingimustele: nõusoleku taotlus on esitatud viisil, mis on muudest küsimustest selgelt eristatav, ning arusaadaval ja lihtsasti kättesaadaval kujul, kasutades selget ja lihtsat keelt. Nõusoleku puhul tuleb silmas pidada ka andmesubjekti õigust nõusolek igal ajal tagasi võtta tulenevalt üldmääruse artikli 7 lg-st 3, kusjuures nõusoleku tagasivõtmine on sama lihtne kui selle andmine.

Samuti saab andmete ülekandmise õigust teostada juhul, kui isikuandmete töötlemine põhineb üldmääruse artikli 6 lg 1 punktis b osutatud andmesubjekti osalusel sõlmitud lepingul. Artikli 6 lg 1 järgi on isikuandmete töötlemine seaduslik juhul, kui isikuandmete töötlemine on vajalik andmesubjekti osalusel sõlmitud lepingu täitmiseks või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele. Üldmäärus ei täpsusta nõudeid andmesubjekti osalusel sõlmitud lepingule. Põhjenduspunkt 40 selgitab üksnes, et töötlemine tuleks lugeda seaduslikuks juhul, kui see on vajalik seoses lepinguga või on tehtud lepingu sõlmimise kavatsusega.[38]

Andmesubjekt ei saa andmete ülekandmise õigust teostada juhul, kui tema isikuandmete töötlemine põhineb muudel üldmääruse artiklis 6 sätestatud õiguslikel alustel, s.o kui tema isikuandmeid töödeldakse juriidilise kohustuse täitmiseks (üldmääruse artikkel 6 lg 1 p c), andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks (üldmääruse artikkel 6

[37] B. Van der Auwermeulen, lk 68; P. Swire and Y. Lagos. Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. – Maryland Law Review 2013/72, Issue 2, lk 338.
[38] Üldmäärus, põhjenduspunkt 40.

lg 1 p d), avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks (üldmääruse artikkel 6 lg 1 p e), ning vastutava töötleja või kolmanda isiku õigustatud huvi korral (üldmääruse artikkel 6 lg 1 p f). Selle sätestab ka üldmääruse artikkel 20 lg 3 teine lause, mille järgi ei kohaldata andmete ülekandmise õigust töötlemise suhtes, mis on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks.

Üldmääruse artiklist 20 ei selgu, kas andmesubjektil on õigus andmete ülekandmisele ka pärast lepingu lõppemist või nõusoleku tagasivõtmist. Artikkel 20 lg 1 p a järgi põhineb töötlemine nõusolekul või lepingul, mille sõnastus viitab, et andmete ülekandmise õiguse eelduseks peaks olema kehtiv nõusolek või leping. Arusaama, et töötlemine saab põhineda just kehtival nõusolekul või lepingul, toetab ka üldmääruse põhjenduspunkt 68: „/.../ See õigus peaks olema kasutatav juhul, kui andmesubjekt esitas isikuandmed omaenda nõusoleku alusel või kui töötlemine on vajalik lepingu täitmiseks /.../.“[39] Eeltoodu põhjal saab väita, et kui andmesubjekti osalusel sõlmitud leping on lõppenud, ei saa töötlemine lepingul põhineda ja seetõttu andmete ülekandmise õigust teostada ei saa. Sama kehtib ka andmesubjekti nõusoleku puhul. Nõusoleku tagasivõtmisel ei saa vastutav töötleja enam sel õiguslikul alusel andmesubjekti isikuandmeid töödelda, mistõttu andmete ülekandmise õigust teostada ei saa.

Nõusoleku tagasivõtmise või lepingu lõppemise korral tuleb vastutaval töötlejal arvestada ka andmekaitseõiguse üldiseid põhimõtteid üldmääruse artiklis 5. Üldmääruse artikli 5 lg 1 p e sisaldub isikuandmete säilitamise piirang, mille järgi võib vastutav töötleja isikuandmeid säilitada kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse. Üldmääruse põhjenduspunkti 39 järgi peaks vastutav töötleja kindlaks määrama tähtajad andmete kustutamiseks või perioodiliseks läbivaatamiseks, et tagada, et isikuandmeid ei säilitataks vajalikust kauem.[40] Niisiis juhul, kui andmesubjekt võtab nõusoleku tagasi või lõpetab lepingu, mille alusel vastutav töötleja tema isikuandmeid töötles, tuleb vastutaval töötlejal silmas pidada andmete säilitamise piirangut ja teha seda üksnes niikaua, kuni on vajalik täita selle andmesubjekti isikuandmete töötlemise eesmärki.

Et nõusoleku tagasivõtmisel või lepingu lõppemisel kaotab andmesubjekt õiguse teostada andmete ülekandmist, võib olla vastuolus andmete ülekandmise õiguse põhilise eesmärgiga anda andmesubjektile suurem kontroll teda puudutavate isikuandmete üle. Samas on ka igal

[39] Üldmäärus, põhjenduspunkt 68.
[40] Üldmäärus, põhjenduspunkt 39.

andmesubjektil igal ajal õigus otsustada, millise vastutava töötlejaga seotud olla. Kui andmesubjekt võtab nõusoleku tagasi või lõpetab lepingu vastutava töötlejaga, ei soovi ta vähemalt eelduslikult jätkata sama vastutava töötleja (kes on nt tema teenusepakkuja) teenuste kasutamist. Nõusoleku või lepingu kehtivuse ajal oli andmesubjektil muude andmesubjekti õiguste kõrval võimalik esitada vastutavale töötlejale taotlus andmete ülekandmiseks. Nõusoleku tagasivõtmise korral on andmesubjektile tagatud õigus nõuda vastutavalt töötlejalt näiteks teda puudutavate isikuandmete kustutamist (üldmääruse artikkel 17 lg 1 p b). Seega ei piira käsitlus, et andmesubjekt saab nõuda vastutavalt töötlejalt andmete ülekandmist üksnes lepingu või nõusoleku kehtimise ajal, ebamõistlikult andmesubjekti võimalust teostada kontrolli teda puudutavate isikuandmete üle.

1.4.2. Isikuandmete automatiseeritud töötlemine

Üldmääruse artikkel 20 lg 1 p b kohaselt on andmesubjektil õigus saada teda puudutavaid isikuandmeid ning edastada need andmed teisele vastutavale töötlejale, kui neid töödeldakse automatiseeritult. Üldmäärus ei defineeri isikuandmete automatiseeritud töötlemise mõistet. Üldmääruse artikkel 4 p 2 sätestab üksnes isikuandmete töötlemise mõiste. See on isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum.

Õiguskirjanduses on selgitatud, et automatiseeritud töötlemine tähendab isikuandmete töötlemist mingi andmetöötluse tehnoloogia abil.[41] Automatiseerimata töötlemine aga tähendab isikuandmete töötlemist täielikult inimese poolt, kasutamata selleks vahendeid või masinaid.[42] Automatiseerimata töötlemine hõlmab üksnes paberkandjal andmeid.[43]

Kokkuvõtlikult tuleb töötlemist pidada automatiseerituks juhul, kui töötlemine toimub tehnoloogia abil ning selle hulka ei kuulu paberkandjal andmed.

1.4.3. Konkreetset andmesubjekti puudutavad isikuandmed

Andmete ülekandmise õiguse kohaldamisalasse kuuluvad ainult konkreetset andmesubjekti puudutavad isikuandmed. Üldmääruse artikkel 4 p 1 järgi on isikuandmeteks igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise idenifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme

[41] P. Voigt, A. von dem Bussche, lk 170.
[42] P. Voigt, A. von dem Bussche, lk 10.
[43] Information Commissioner’s Office. Guide to the General Data Protection Regulation (GDPR) 2018, lk 129.

füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.

Isikuandmete mõistet tõlgendatakse laialt. „Igasuguse teabe“ alla kuulub teave, mis ei ole piiritletud isikliku teabega või teabega, mida hoitakse mõnel kindlal andmekandjal.[44] Euroopa Kohus leidis *Satamedia* otsuses, et ka avalikustatud teave on hõlmatud „isikuandmete“ mõistega.[45] Teave peab olema füüsilise isiku kohta, mida tõlgendatakse samuti laialt. Näiteks võib see isegi hõlmata teavet mõne objekti kohta, nt maja hinda, seni kuni see annab teavet tuvastatud või potentsiaalselt tuvastatava füüsilise isiku kohta.

Eriti laiaks muudab isikuandmete mõiste see, et lisaks tuvastatud isikule võib isik olla ka potentsiaalselt tuvastatav. See tähendab, et isegi kui isiku identiteet ei ole otseselt teada, on isikuandmetega tegemist seni, kuni leidub võimalusi isiku identiteedi kindlakstegemiseks.[46] Selleks tuleb arvesse võtta kõiki viise, mida isiku identiteedi tuvastamiseks võidakse mõistlikkuse piires kasutada vastutava töötleja või mis tahes muu isiku poolt.[47]

Andmete ülekandmise õiguse kohaldamisalasse ei kuulu andmed, mis on anonüümsed või ei puuduta andmesubjekti. Kohaldamisalasse kuuluvad siiski pseudonüümi all esitatud andmed, kui neid on võimalik selgelt andmesubjektiga seostada.[48] Pseudonüümi all esitatud andmeid on võimalik selgelt andmesubjektiga seostada näiteks juhul, kui andmesubjekt on esitanud vastava identifitseerimistunnuse artikli 11 lg 2 järgi,[49] ehk esitanud enda tuvastamist võimaldavat lisateavet vastutavale töötlejale.

1.4.4. Andmesubjekti enda poolt esitatud isikuandmed

Andmesubjektil on õigus üksnes nende andmete ülekandmisele, mida loetakse andmesubjekti enda poolt vastutavale töötlejale esitatud isikuandmeteks. Et kindlaks määrata, milliseid andmeid loetakse andmesubjekti enda esitatud isikuandmeteks, eristatakse kolme võimalikku lähenemisviisi.

(a) Kitsa lähenemisviisi kohaselt on „esitatud isikuandmeteks“ andmesubjekti poolt vabatahtlikult või aktiivselt avaldatud isikuandmed, nt kui ta on täitnud vormi või vastanud

[44] H. Kranenborg. Art 8 – Protection of Personal Data. – S. Peers jt. The EU Charter of Fundamental Rights: A Commentary. Hart Publishing 2014, lk 243.
[45] EKo C-73/07 *Satamedia*, p 35, kus Euroopa Kohus leidis, et selles küsimuses nimetatud andmed, mis puudutavad teatavate niisuguste füüsiliste isikute ees- ja perekonnanime, kelle tulu ületab teatava piiri, ning eelkõige nende kapitali- ja palgatulu 100-eurose täpsusega, on isikuandmed direktiivi artikli 2 punkti a tähenduses, kuna tegemist on „teabega tuvastatud või tuvastatava füüsilise isiku kohta”.
[46] H. Kranenborg, lk 243.
[47] H. Kranenborg, lk 243; Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, põhjenduspunkt 26.
[48] Artikli 29 töörühm, lk 9.
[49] Artikli 29 töörühm, lk 9.

küsimustikule.[50] Interneti teel vastutava töötleja kui teenusepakkuja juures kasutajaks registreerimisel on sellisteks isikuandmeteks näiteks andmesubjekti nimi, sugu, sünnikuupäev jm isiklik teave. Samuti loetakse andmesubjekti esitatud isikuandmeteks ka näiteks andmesubjekti poolt üleslaetud faile, pilte või postitusi.[51] Üldmääruse artikkel 4 p 1 sätestab, et isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti") kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada. Seega, mis tahes andmesubjekti esitatud andmed peavad andma üldmääruse artikli 4 p-st 1 lähtudes sellist teavet, mille kaudu andmesubjekt on tuvastatud või teda on võimalik otseselt või kaudselt tuvastada.

(b) Laiema tõlgenduse kohaselt on andmesubjekti esitatud isikuandmeteks ka „passiivselt esitatud" isikuandmed või andmesubjekti kohta vastutava töötleja võimaldatavaid seadmeid või teenuseid kasutades saadud isikuandmed.[52] Passiivselt esitatud isikuandmeteks on andmed, mille vastutav töötleja on andmesubjekti kohta kogunud andmesubjekti nõusoleku või andmesubjekti osalusel sõlmitud lepingu alusel. Nende all peetakse silmas algandmeid, mille on kogunud näiteks arvesti andmesubjekti majapidamises, tervise- või spordijälgimisseadmete abil kogutud südamelöögi andmeid või otsinguajaloo andmeid.[53] Oluline on aga märkida, et andmed, mille vastutav töötleja on ise loonud andmesubjekti esitatud isikuandmete analüüsimise tulemusena, loetakse vastutava töötleja andmeteks ning need andmed ei ole andmete ülekandmise õigusega hõlmatud.[54] Vastutava töötleja poolt loodud andmeteks on näiteks andmesubjekti esitatud andmete põhjal andmesubjekti kohta loodud hinnangud, profiilid, skoorid jne[55] (terviseanalüüs või krediidiskoor)[56]. Laiem tõlgendus andmesubjekti esitatud isikuandmetest hõlmab seega nii andmesubjekti enda vabatahtlikult või aktiivselt esitatud isikuandmeid ja andmesubjekti kohta passiivselt kogutud isikuandmeid, mis ei ole loodud vastutava töötleja poolt andmete analüüsimise tulemusena.

(c) Kõige laiema tõlgenduse kohaselt hõlmavad andmesubjekti poolt esitatud isikuandmed kõiki isikuandmeid, mida vastutav töötleja andmesubjekti kohta lepingu või nõusoleku alusel töötleb. Selline lähenemine põhineb ideel, et andmesubjekt on nõusoleku andmise või lepingu

[50] I. Graef jt. Data Portability and Data Control: Lessons from an Emerging Concept in EU Law. – German Law Journal 2018/19, No. 6, lk 1372.
[51] B. Van der Auwermeulen, lk 69; P. Swire, Y. Lagos, lk 347 .
[52] I. Graef jt 2018, lk 1372.
[53] J. Schrey, lk 144.
[54] J. Schrey, lk 144.
[55] I. Graef jt 2018, lk 1373.
[56] J. Schrey, lk 144.

sõlmimise teel nõustunud andmete töötlemisega ning sellest tulenevalt on kõik andmesubjekti isikuandmed andmesubjekti poolt vastutavale töötlejale esitatud isikuandmeteks.[57]

Artikli 29 töörühm on andmete ülekandmise õiguse kohta koostatud suunistes valinud eelnevalt punktis (b) kirjeldatud laiema tõlgenduse, selgitades, et „andmesubjekti poolt esitatud andmeid" tuleks tõlgendada laialt ning üksnes järeldatud või tuletatud andmed tuleb andmete ülekandmise õiguse kohaldamisalast välja arvata.[58] Andmed, mille vastutav töötleja on ise andmesubjekti esitatud andmetest tuletanud, ei kuulu andmesubjekti poolt esitatud andmete hulka ega ole andmete ülekandmise õiguse objektiks. Seega ei ole andmete ülekandmise õigusega hõlmatud sellised andmed, mis tulenevad andmesubjekti tegevuse või käitumise hilisemast analüüsimisest.[59]

Andmesubjekti poolt vastutavale töötlejale esitatud andmete määratlemisel saab tuua huvitava näite töösuhete valdkonnast, kus on muutunud tavapäraseks see, et tööandja jälgib vähemal või suuremal määral töötaja telefonikasutust, e-kirjavahetust ja internetikasutust. Võimalik on ka, et töötajate jälgimiseks on töökohale paigaldatud jälgimiskaamerad. Kas nimetatud vahendite teel töötajate kohta kogutud info saab olla käsitletav töötaja poolt tööandjale esitatud andmetena ning kas töötaja peaks saama selliseid andmeid üle kanda?

Töötaja kui andmesubjekti telefonikõned, e-kirjad ja internetikasutus on kõik käsitletavad töötaja enda esitatud andmetena, sest need tekivad töötaja aktiivse tegevuse tulemusena. Need kuuluvad eelnevalt punktis a nimetatud kitsa määratluse alla.

Töökohale paigaldatud jälgimiskaamera salvestis seevastu tekib aga passiivselt, st jälgimisseadme kaudu andmete kogumise tulemusena. Artikli 29 töörühm on seisukohal, et andmesubjekti jälgimise ja tema tegevuse salvestamise kaudu (nt südamelööke salvestav rakendus või sirvimiskäitumise jälgimiseks kasutatav tehnoloogia) kogutud andmeid tuleks samuti käsitada tema „esitatud" andmetena isegi juhul, kui neid ei ole edastatud aktiivselt ja teadlikult.[60] Seega, eelnevalt punktis b käsitletud laia tõlgenduse põhjal kuuluvad jälgimisseadme abil töötaja kui andmesubjekti kohta kogutud andmed vastutavale töötlejale esitatud andmete hulka, kuni vastutav töötleja ei ole nimetatud andmeid mingil viisil analüüsinud.

Juhul, kui täidetud on ka kõik muud andmete ülekandmise õiguse teostamise eeldused, saab töötaja eeltoodud näite põhjal andmete ülekandmise õigust teostada nii telefonikõnede, e-

[57] I. Graef jt 2018, lk 1372.
[58] Artikli 29 töörühm, lk 10.
[59] Artikli 29 töörühm, lk 11.
[60] Artikli 29 töörühm, lk 10.

kirjade kui ka internetikasutuse osas, samuti ka tema kohta jälgimisseadme abil kogutud isikuandmete osas.

1.4.5. Andmete ülekandmise õiguse teostamine ei kahjusta teiste isikute õigusi ja vabadusi

Üldmääruse artikli 20 lg 4 sätestab, et lõikes 1 osutatud õigus ei kahjusta teiste isikute õigusi ja vabadusi. Tegemist on andmete ülekandmise õiguse kohaldamiseks ette nähtud „tasakaalustamisklausliga", mille eesmärk on tagada, et andmete ülekandmise õiguse rakendamine ei tekitaks teiste isikute õigustele ja vabadustele põhjendamatut kahju ega piiraks teiste isikute õigusi ja vabadusi ebaseaduslikult.[61]

Üldmääruse artikli 20 lg 4 tõlget inglise keelest eesti keelde ei saa aga autori hinnangul pidada õnnestunuks. Üldmääruse eestikeelses tekstis on artikkel 20 lg 4 tõlgitud kui „lõikes 1 osutatud õigus ei kahjusta teiste isikute õigusi ja vabadusi" (ingl k „*The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others*"). Autori hinnangul esineb eestikeelses versioonis tõlkeviga. Ingliskeelses sättes kasutatakse käskivat kõneviisi *shall not* (eesti keeles *ei tohi*), mida aga eestikeelses versioonis ei väljendu.

Eesti- ja ingliskeelseid sätteid võrreldes on neil täiesti erinev tähendus. Eestikeelsest tekstist, mille kohaselt lõikes 1 osutatud õigus ei kahjusta teiste isikute õigusi ja vabadusi, võiks mõistlikult järeldada, et andmete ülekandmise õigust saab teostada piiramatult, pööramata tähelepanu teiste isikute õigustele ja vabadustele, sest nende kahjustumine on andmete ülekandmise õiguse teostamisel üldmääruse artikli 20 lg 4 alusel igal juhul välistatud. Ingliskeelsest tekstist, et lõikes 1 osutatud õigus ei tohi kahjustada teiste isikute õigusi ja vabadusi, järeldub aga vastutava töötleja kohustus tagada, et andmete ülekandmise õigus kellegi teise õigusi ja vabadusi ei kahjustaks. Sätte eesmärk peaks olema kaitsta teiste isikute õigusi ja vabadusi, mitte rõhutada andmete ülekandmise õiguse piiramatut teostamist. Üldmääruse põhjenduspunkt 68 (ka eesti keelde tõlgituna) viitab samuti sellele, et andmete ülekandmise õigus ei tohiks piirata teiste isikute õigusi ja vabadusi.[62] Seega on autor seisukohal, et korrektne üldmääruse artikli 20 lg 4 tõlge oleks: lõikes 1 osutatud õigus ei tohi kahjustada teiste isikute õigusi ja vabadusi.

Lisaks tuleb veel selgitada, kas üldmääruse artikli 20 lg-s 4 sätestatud õiguste ja vabaduste kahjustamise all on silmas peetud õiguste riivet või rikkumist. Õigusteoorias eristatakse rangelt põhiõiguste riivet ja rikkumist. R. Maruste määratluse järgi saab põhiõiguste riivet ja rikkumist

[61] P. de Hert jt, lk 198.
[62] Üldmäärus, põhjenduspunkt 68.

eristada järgmiselt: „Kui riive on tuvastatud, siis järgmine samm on selgitada, kas riivega ka põhiõigusi ja vabadusi on (tegelikult) rikutud. Mitte iga riive ei tähenda automaatselt õiguste ja vabaduste rikkumist. Riive võib olla olemuselt formaalne või materiaalne (sisuline e tegelik). Samuti tuleb riive mõiste hoida rangelt lahus põhiõiguste ja vabaduste rikkumise mõistest. Kui riive on kõikide üldtunnustatud kriteeriumite järgi seaduslik ja õigustatud, on see küll sekkumine, kuid mitte veel rikkumine.“[63] R. Alexy järgi on põhiõiguse riive põhiõiguse rikkumine ainult siis, kui see on formaalselt või materiaalselt põhiseaduse vastane.[64]

Eeltoodu valguses tuleks asuda seisukohale, et üldmääruse artikkel 20 lg-s 4 on kahjustamise all silmas peetud siiski reaalset õiguste rikkumist, mitte üksnes õiguste riivet. Üldmääruse ingliskeelses versioonis kasutatav termin *adversely affect* tähistab õiguste kahjustumist, mida kinnitab keelekasutus Euroopa Kohtu praktikas: nt Digital Rights Ireland lahendis[65] on kohus eristanud inglise keelest eesti keelde tõlgituna õiguste rasket riivet (*serious interference*) ja õiguste kahjustumist (*adversely affect*). Seega tähistab üldmääruse artikli 20 lg-s 4 sätestatud õiguste kahjustamine õiguste rikkumist, mitte riivet.

1.5.Vastutava töötleja õigused ja kohustused seoses andmete ülekandmise õigusega

1.5.1. Andmeid saatva vastutava töötleja õigused ja kohustused

Vastutav töötleja peab andmesubjektile esitama andmed struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul (üldmääruse artikkel 20 lg 1). Struktureeritud vorming tähendab andmete funktsionaalset ja hõlpsat ülekandmist võimaldavat vormingut.[66] Üldkasutatava ehk avatud vormingu all peetakse silmas vorminguid, mis ei ole seotud kitsamalt kasutatava kommertstarkvaraga.[67] Masinloetaval kujul on andmed juhul, kui see võimaldab andmeid lugeda arvutisüsteemis või veebibrauseris ja mis seeläbi võimaldavad andmete automaatset töötlemist.[68]

Andmesubjektil on õigus andmed edastada teisele vastutavale töötlejale, ilma et seda takistaks vastutav töötleja, kellele on isikuandmed esitatud (artikkel 20 lg 1). Vastutaval töötlejal on seega keelatud selliste vormingute kasutamine, millega oleks andmete ülekandmine tehniliselt takistatud. Nimetatud kohustuse eesmärgiks on vältida vastutava töötleja poolt andmete

[63] R. Maruste. Konstitutsionalism ning põhiõiguste ja –vabaduste kaitse. Tallinn: Juura 2004, lk 246-247.
[64] R. Alexy. Põhiõigused Eesti põhiseaduses. – Justiitsministeeriumi juriidilise ekspertiisi komisjon, 1997, lk 40.
[65] EKo liidetud kohtuasjades C-293/12 ja C-594/12, *Digital Rights Ireland Ltd. v Iirimaa*.
[66] Struktureeritud vorminguks peetakse näiteks RDL-i või XML-i, kuid mitte PDF-i vormingut. – B. Van der Auwermeulen, lk 71; P. Swire, Y. Lagos, lk 346.
[67] Andmekaitse Inspektsioon. Isikuandmete töötleja üldjuhend 19.03.2019, lk 36.
[68] B. Van der Auwermeulen, lk 71.

taaskasutamise takistamist. Vastutavalt töötlejalt eeldatakse, et ta ei väljasta andmesubjektile andmeid sellises vormis, mida ei saa taaskasutada.[69]

Vastutav töötleja on kohustatud andmed esitama andmesubjektile tasuta (üldmääruse artikkel 12 lg 5). Kui andmesubjekti taotlused on selgelt põhjendamatud või ülemäärased, eelkõige oma korduva iseloomu tõttu, võib vastutav töötleja kas küsida mõistlikku tasu, võttes arvesse halduskulu, mis kaasneb teabe esitamise või teavitamise või taotletud meetmete võtmisega, või keelduda taotletud meetmete võtmisest. Vastutaval töötlejal lasub kohustus tõendada, et taotlus on selgelt põhjendamatu või ülemäärane.

Vastutaval töötlejal on üldmääruse artikli 12 lg-st 3 tulenevalt kohustus esitada andmesubjektile tarbetu viivituseta, kuid mitte hiljem kui ühe kuu jooksul pärast taotluse saamist teave artiklite 15-22 kohase taotluse alusel võetud meetmete kohta. Seda ajavahemikku võib vajaduse korral pikendada kahe kuu võrra, võttes arvesse taotluse keerukust ja hulka. Vastutav töötleja teavitab andmesubjekti igast taolisest pikendamisest ja viivituse põhjustest ühe kuu jooksul alates taotluse saamisest. Kui andmesubjekt esitab taotluse elektrooniliselt, esitatakse ka teave võimaluse korral elektrooniliselt, kui andmesubjekt ei taotle teisiti.

Siiski ei ole vastutav töötleja kohustatud kasutusele võtma või töös hoidma selliseid töötlemise süsteeme, mis on „tehniliselt ühilduvad“. Üldmääruse põhjenduspunkt 68 sätestab sõnaselgelt: „/.../ Andmesubjekti õigus edastada või saada teda puudutavaid isikuandmeid ei peaks tekitama vastutavatele töötlejatele kohustust võtta kasutusele või hoida töös tehniliselt ühilduvaid andmetöötlussüsteeme. /.../“[70] Majanduslikust aspektist vaadatuna ei oleks autori hinnangul vastutavatelt töötlejatelt ühilduvate süsteemide kasutuselevõtmine või töös hoidmine ka mõistlik, sest vastutavad töötlejad on süsteemide ja andmebaaside struktuuride väljaarendamiseks kulutanud raha ja seeläbi soovinud saada majanduslikku eelist konkurendi ees. Ühilduvate süsteemide loomine tähendaks, et vastutav töötleja peab tegema täiendavaid väljaminekuid juba olemasolevate ja välja arendatud süsteemide muutmiseks. Samas, lähtudes andmekaitse eesmärkidest, võivad ühilduvate süsteemide puudumine ja liialt keerulised andmete ülekandmise vormingud viia lõppastmes selleni, et andmesubjektil ei olegi automaatsel teel võimalik andmeid teise vastutava töötleja juurde üle kanda, sest vastutavate töötlejate poolt kasutatavad süsteemid ja andmebaaside struktuurid ei võimalda andmeid ühest süsteemist teise üle kanda.

[69] B. Van der Auwermeulen, lk 71.
[70] Üldmäärus, põhjenduspunkt 68.

Artikli 29 töörühm on välja toonud, et andmeid saatev vastutav töötleja ei vastuta andmeid vastuvõtva vastutava töötleja poolt andmekaitsenõuete täitmise eest. Küll aga peab andmete ülekandmise korral andmeid saatev vastutav töötleja seadma turvameetmed, et kontrollida, et andmeid vastuvõttev vastutav töötleja tegutseb andmesubjekti nimel.[71] Sellist kohustust vastutavale töötlejale üldmääruse tekst ei sätesta. Artikli 29 töörühm selgitab täiendavalt, et näiteks saavad vastutavad töötlejad seada sisse menetlused, millega tagatakse, et edastatakse ka tegelikult sellist liiki isikuandmeid, mida andmesubjekt soovib edastada. Selleks võib hankida andmesubjekti kinnituse kas enne andmete edastamist või varem, töötlemiseks algse nõusoleku andmise või lepingu sõlmimise ajal.[72]

Samuti on vastutaval töötlejal kohustus tagada isikuandmete töötlemise läbipaistvus. Üldmääruse põhjenduspunkt 58 selgitab, et „Läbipaistvuse põhimõte eeldab, et üldsusele või andmesubjektile suunatud teave on kokkuvõtlik, lihtsalt kättesaadav ja arusaadav ning selgelt ja lihtsalt sõnastatud /.../“.[73] Läbipaistvuse tagamiseks tuleb vastutaval töötlejal esitada andmesubjektile artiklites 13 ja 14 osutatud teave (sh teave isikuandmete vastutava töötleja kohta, isikuandmete töötlemise eesmärgi ja õigusliku aluse kohta, asjakohasel juhul teave andmekaitseametniku kontaktandmete kohta, õigustatud huvil põhineva töötlemise korral vastutava töötleja või kolmanda isiku õigustatud huvide kohta jms). Ühtlasi tuleb vastutaval töötlejal andmesubjekti teavitada artiklite 15-22 ja 34 kohaselt isikuandmete töötlemisest (andmesubjekti õiguste alusel meetmete võtmisest või isikuandmetega seotud rikkumisest) kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt (artikkel 12 lg 1).

1.5.2. Andmeid vastuvõtva vastutava töötleja õigused ja kohustused

Andmeid vastuvõttev vastutav töötleja (edaspidi nimetatud kui uus vastutav töötleja) peab tagama kõikide üldmäärusest tulenevate kohustuste täitmise, et tagada andmesubjekti isikuandmete kaitse.

Lisaks üldmääruse artiklitest 12, 13, 14 ja 20 tulenevatest kohustustest, mida on kirjeldatud ülal (vt käesoleva töö alapeatükk 1.5.1), on uue vastutava töötleja kohta artikli töörühma juhendis eraldi välja toodud, et uus vastutav töötleja peab tagama, et ülekantavad andmed on asjakohased ja neid on uue andmetöötluse seisukohalt minimaalselt.[74] Minimaalsuse ja asjakohasuse nõuded tulenevad üldmääruse artiklist 5. Artikli 5 lg 1 p b sätestab eesmärgi piirangu, st isikuandmeid

[71] Artikli 29 töörühm, lk 6; L. Feiler, N. Forgó, M. Weigl. The EU General Data Protection Regulation (GDPR): A Commentary. Globe Law and Business 2018, lk 130.
[72] Artikli 29 töörühm, lk 6.
[73] Üldmäärus, põhjenduspunkt 58.
[74] Artikli 29 töörühm, lk 6.

kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus. Artikli 5 lg 1 p c sätestab võimalikult väheste andmete kogumise põhimõtte: isikuandmed on asjakohased, olulised ja piiratud sellega, mis on nende töötlemise eesmärgi seisukohalt vajalik.

Artikli 29 töörühm on veel selgitanud: „Vastuvõtvast organisatsioonist saab kõnealuste isikuandmete puhul uus vastutav töötleja ja ta peab järgima isikuandmete kaitse üldmääruse artiklis 5 sätestatud põhimõtteid. Seepärast peab uus vastuvõttev vastutav töötleja enne mis tahes taotlust ülekantavate andmete edastamise kohta täpsustama kooskõlas artiklis 14 sätestatud läbipaistvusnõuetega selgelt ja otseselt uue töötlemise eesmärgi. Nagu mis tahes muu tema vastutusel toimuva andmete töötlemise puhul peaks vastutav töötleja kohaldama artiklis 5 sätestatud põhimõtteid, nagu seaduslikkus, õiglus ja läbipaistvus, eesmärgi piirang, võimalikult väheste andmete kogumine, õigsus, usaldusväärsus ja konfidentsiaalsus, säilitamise piirang ning vastutus.“[75]

Kuigi üldmääruse artikkel 20, mis reguleerib andmete ülekandmise õigust, ei sätesta otsesõnu uuele vastutavale töötlejale kohustust andmetega sisuliselt tutvuda, tuleb sellisel juhul lähtuda põhimõttest, et uuel vastutaval töötlejal on kohustus järgida kõiki üldmääruse artiklis 5 sätestatud isikuandmete töötlemise põhimõtteid. Näiteks eelnevalt mainitud võimalikult väheste andmete kogumise põhimõtte (artikkel 5 lg 1 p c) kohaselt peab uus vastutav töötleja kindlaks tegema, et talle üle kantud andmed on asjakohased. Seda saab ta aga teha üksnes juhul, kui ta saadud andmetega ka sisuliselt tutvub. Samamoodi võib eesmärgi piirangust (artikkel 5 lg 1 p b) lähtudes väita, et uus vastutav töötleja peab talle üle kantud andmetega sisuliselt tutvuma selleks, et määratleda saadud andmete töötlemise eesmärk. Artikli 29 töörühma põhimõtet järgides asun seisukohale, et uuel vastutaval töötlejal tuleb saadud andmetega sisuliselt tutvuda.

Käesolevas töös analüüsitakse järgnevas peatükis ka olukorda, kus andmete ülekandmisel kantakse ühes andmesubjekti isikuandmetega uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed. Sellel on tähendus uue vastutava töötleja artiklist 14 tulenevate kohustuste mõistmiseks. Artikli 29 töörühma suunistest lähtuvalt tuleb uuel vastutaval töötlejal täpsustada kooskõlas artiklis 14 sätestatud läbipaistvusnõuetega selgelt ja otseselt uus töötlemise eesmärk. Üldmääruse artiklis 14 sisalduvad läbipaistvusnõuded sisaldavad mh ka uue vastutava töötleja kohustust teavitada andmesubjekti tema isikuandmete töötlemisest vastutava töötleja poolt, kui andmed ei ole saadud andmesubjektilt. Kui andmesubjekti esitatud taotluse alusel kantakse uue

[75] Artikli 29 töörühm, lk 7.

vastutava töötleja juurde üle andmed, milles sisalduvad ka kolmanda isiku isikuandmed, siis muutub kolmas isik uue vastutava töötleja silmis andmesubjektiks. Kuna kolmanda isiku andmed ei ole tema enda esitatud, on uue vastutava jaoks kolmanda isiku isikuandmed saadud artikli 14 mõttes mujalt kui andmesubjektilt. Seepärast peab uus vastutav töötleja täitma kohustuse teavitada andmesubjekti tema isikuandmete töötlemisest uue vastutava töötleja poolt.

1.6.Isikuandmete turvalisus andmete ülekandmisel

Peamine turvarisk andmete ülekandmisel on oht, et vastutav töötleja ei suuda korrektselt identifitseerida andmesubjekti isikut ja väljastab andmed isikule, keda andmed tegelikult ei puuduta. Nii on võimalik, et andmete ülekandmise õigust kuritarvitades püütakse vastutavalt töötlejalt saada kellegi teise isikuandmeid. Juba 2013. aastal juhiti õiguskirjanduses tähelepanu sellele, et üldmääruse regulatsiooni kavandamisel tuleb viia identiteedivarguste risk miinimumi.[76]

Turvariskide oht on andmete ülekandmise õiguse puhul võrreldes teiste andmesubjekti õigustega eriti tugev. Identiteedivarguse korral on võimalik saada koopia vastutava töötleja juures kogutud andmesubjekti isikuandmetest, kanda need üle teise vastutava töötleja juurde või paluda vastutavalt töötlejalt andmete otse ülekandmist teise vastutava töötleja juurde. See võib tähendada ligipääsu saamist mitme aasta või koguni aastate jooksul andmesubjekti poolt esitatud isikuandmetele.[77]

Et teha kindlaks, millised võimalused on vastutaval töötlejal taotluse esitanud isiku identifitseerimiseks ning kas üldmäärus näeb ette erinõudeid, kas ja kuidas peab vastutav töötleja andmete ülekandmise taotluse esitanud isiku kindlaks tegema, on asjakohased sätted üldmäärusest järgnevad.

Üldmääruse artikkel 12 lg 2 sätestab:

Vastutav töötleja aitab kaasa artiklite 15–22 kohaste andmesubjekti õiguste (vt lähemalt käesoleva töö alapeatükk 1.2) *kasutamisele. Artikli 11 lõikes 2 osutatud juhtudel ei keeldu vastutav töötleja meetmete võtmisest andmesubjekti taotlusel tema artiklite 15–22 kohaste õiguste kasutamiseks, välja arvatud juhul, kui vastutav töötleja tõendab, et ta ei suuda andmesubjekti tuvastada.*

Üldmääruse artikkel 12 lg 6 sätestab:

[76] I. Graef 2015, lk 507; P. Swire, Y. Lagos, lk 373-375.
[77] P. Swire, Y. Lagos, lk 374.

Kui vastutaval töötlejal on põhjendatud kahtlused artiklites 15–21 osutatud taotlust esitava füüsilise isiku identiteedi suhtes, võib vastutav töötleja nõuda andmesubjekti isiku tuvastamiseks vajaliku täiendava teabe esitamist, piiramata seejuures artikli 11 kohaldamist.

Üldmääruse artikkel 11 lg 2 sätestab:

2. Kui vastutav töötleja on käesolevas artikli lõikes 1 osutatud juhtudel võimeline tõendama, et ta ei suuda andmesubjekti tuvastada, teavitab ta vastavalt andmesubjekti, kui see on võimalik. Sellistel juhtudel ei kohaldata artikleid 15–20, välja arvatud juhul, kui andmesubjekt esitab enda tuvastamist võimaldavat lisateavet, et kasutada nende artiklite kohaseid õigusi.

Välja toodud sätteid analüüsides ei sätesta üldmäärus otsesõnu vastutavale töötlejale kohustust andmesubjekti isiku tuvastamiseks, kuid tulenevalt artikli 12 lg 2 sõnastusest on see vajalik, kui vastutav töötleja keeldub andmete ülekandmise õiguse kasutamisest. Et aga üldmääruse artikkel 12 lg 2 on ainus säte üldmääruses, mis annab vastutavale töötlejale sõnaselgelt õiguse otsustada, kas esitatud andmete ülekandmise taotlus rahuldada või mitte, ei saa vastutav töötleja sellist kaalutlust teostada enne, kui ta on taotluse esitanud isiku tuvastanud.

Minu hinnangul muutuks üldmääruse artikli 12 lg 2 sisutühjaks ja vastutaval töötlejal ei oleks võimalik kaalutleda, kas taotlus rahuldada või mitte, kui vastutav töötleja ei tuvastaks isikut, kes taotluse esitas. Ainult juhul kui vastutav töötleja teeb katse tuvastada taotluse esitanud isik, mille tulemusena isikut ei ole võimalik tuvastada, on tal üldmääruse artikli 12 lg 2 alusel õigus keelduda andmesubjekti taotluse rahuldamisest. Lähtudes artikli 12 lg 2 mõttest, tuleks tunnustada vastutava töötleja kohustust andmete ülekandmise taotluse esitanud isiku tuvastamiseks.

Vastutava töötleja kohustust tuvastada taotluse esitanud isik kinnitab ka üldmääruse artiklist 12 lg 2 tulenev vastutava töötleja tõendamiskohustus. Nimelt peab vastutav töötleja meetmete võtmisest keeldumisel tõendama, et ta ei suuda andmesubjekti tuvastada. Sättest tulenevat tõendamiskoormist on vastutaval töötlejal võimalik täita ainult juhul, kui ta on teinud katse andmesubjekti isikut tuvastada.

Eelnevast selgub, et vastutaval töötlejal on õigus keelduda andmesubjekti taotletud meetmete võtmisest, kui vastutaval töötlejal ei ole võimalik andmesubjekti tuvastada. See kehtib aga eeldusel, et andmesubjekt ei esita täiendavat infot enda isiku kindlakstegemiseks. Nimelt teeb artikkel 12 lg 2 viite artikkel 11 lg-le 2. Artikli 11 lg-st 2 tuleneb, et vastutav töötleja teavitab andmesubjekti, kui tal ei ole võimalik tema isikut tuvastada ja annab isikule võimaluse esitada

tuvastamist võimaldavat lisateavet. Üksnes juhul kui ka lisateabe alusel ei ole võimalik isikut tuvastada, saab vastutav töötleja keelduda andmesubjekti taotletud meetmete võtmisest.

Sellest järeldub, et üldmääruse artiklitest 11 lg 2 ja 12 lg 2 tuleneb koosmõjus, et vastutaval töötlejal on õigus keelduda andmesubjekti esitatud artiklite 15-20 kohase taotluse rahuldamisest, kui vastutav töötleja ei suuda tuvastada andmesubjekti isikut. Seda eeldusel, et andmesubjekt ei esita lisateavet, mis võimaldab tema isiku tuvastada.

Seetõttu tuleks minu hinnangul vastutavatel töötlejatel vastu võtta automaatne autentimismenetlus[78] puhuks, kui andmesubjektid soovivad teostada üldmääruses sätestatud andmesubjekti õigusi (vt lähemalt käesoleva magistritöö alapunkt 1.2). See oleks kooskõlas ka üldmääruse artikliga 32, mis suunab vastutavaid töötlejaid rakendama turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid, võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning arvestades isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja suurusega ohte füüsiliste isikute õigustele ja vabadustele. Arvestades identiteedivarguste ohtu ja sellest tuleneda võivat kahju andmesubjekti õigustele ja vabadustele, on autentimismenetluse kehtestamine vastutava töötleja poolt üldmääruse artikli 32 kohase meetmena igati põhjendatud andmete ülekandmise õiguse puhuks.

Automaatne autentimismenetlus võiks olla vastutava töötleja poolt rakendatav selline tehniline lahendus, kus andmesubjekt peab enda isiku täiendavalt tuvastama. Näiteks kui andmesubjekt esitab andmete ülekandmise taotluse olles vastavasse süsteemi sisse logitud, tuleks andmesubjektil uuesti sisestada kasutajatunnus ja salasõna.[79] Lisaks peab vastutav töötleja üldmääruse artiklist 32 tulenevalt arvesse võtma teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid, isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke jne, rakendades ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid. Eeltoodu valguses on soovitatud kasutajatunnuse ja salasõna süsteemi perioodilist uuendamist.[80] Samuti on võimalik, et tulenevalt erinevate internetikeskkondade eripäradest

[78] Autentimine tähendab sellist protseduuri, milles isikul on võimalik tõendada, et ta omab kindlat identiteeti ja/või on õigustatud teatud tegevuste läbiviimiseks. /…/ Autentida saab nt küsides isikult teavet, mida peaks teadma ainult isik, kellel on kindle identiteet või volitus, nt isiklik identifitseerimisnumber (PIN) või parool /…/, samuti elektroonilise suhtluse puhul elektrooniline allkiri. – European Union Agency for Fundamental Rights and Council of Europe. Handbook on European data protection law 2018 edition, lk 83 ja 95.
[79] P. B. Lambert. Understanding the New European Data Protection Rules. Taylor & Francis Group 2018, lk 46-47.
[80] Information Commissioner's Office, lk 224.

võib teatud juhtudel olla kohane rakendada mõnda muud autentimismenetlust peale salasõna kasutamise, mis aitab paremini tagada andmete töötlemise turvalisust.[81]

Kui andmete ülekandmise õiguse teostamist sooviv andmesubjekt ei läbi autentimismenetlust edukalt, võiks vastutav töötleja tema taotluse eraldi läbi vaadata. Tuginedes üldmääruse artikkel 11 lg-le 2, peaks vastutav töötleja võimaldama andmesubjektil esitada lisateavet, et andmesubjekt tuvastada. Kui ka see ei õnnestu, saab vastutav töötleja keelduda andmete ülekandmise õiguse teostamisest. Selline lahendus on kooskõlas ka artikli 29 töörühma arvamusega, et kui andmesubjekt esitab lisateavet, mis võimaldab teda tuvastada, siis ei või vastutav töötleja keelduda taotluse täitmisest.[82]

Taotluse esitanud andmesubjekti tuvastamiseks automaatse autentimismenetluse kasutuselevõtt aitab ühtlasi vastutaval töötlejal täita tõendamiskoormist andmesubjekti tuvastamise kohta. Vastutaval töötlejal lasub tõendamiskoormis, et ta ei suuda andmesubjekti tuvastada, kui ta soovib üldmääruse artikli 12 lg 2 alusel jätta andmesubjekti esitatud taotluse rahuldamata. Vastutava töötleja tõendamiskoormise täitmise lihtsustamiseks tuleb luua selline tehniline lahendus, mis dokumenteerib kõik autentimismenetluse etapid ning näitab ära, kui andmesubjekti isik ei ole tuvastatav.

Juhul kui vastutav töötleja palub andmesubjektilt lisateavet tema isiku tuvastamiseks, tuleb vastutaval töötlejal arvestada kõikide isikuandmete töötlemise põhimõtetega üldmääruse artiklist 5 tulenevalt. Ka artikli 29 töörühm on selgitanud, et põhimõtteliselt ei saa asjaolu, et vastutav töötleja saab taotleda isiku identiteedi tuvastamiseks lisateavet, tuua kaasa liigseid nõudmisi ega selliste isikuandmete kogumist, mis ei ole asjakohased või vajalikud isiku ja taotletavate isikuandmete vahelise seose kinnitamiseks.[83] Seega tuleb vastutaval töötlejal isiku identiteedi tuvastamisel lähtuda eelkõige sellistest isikuandmete töötlemise põhimõtetest nagu eesmärgipärasus ja minimaalsus ja küsida andmesubjektilt üksnes sellist andmesubjekti puudutavat lisateavet, mis on vältimatult vajalik.

Lisaks eeltoodule on erialakirjanduses väljendatud arvamust, et üldmääruse artiklis 20 sätestatud tingimus, et vastutav töötleja edastab andmed otse teisele vastutavale töötlejale, kui see on tehniliselt teostatav, lisab täiendava riski andmete ülekandmise õiguse turvalisusesse.[84]

[81] Information Commissioner's Office, lk 224.
[82] Artikli 29 töörühm, lk 13.
[83] Artikli 29 töörühm, lk 14.
[84] P. Swire, Y. Lagos, lk 374.

Seepärast tuleks vastutaval töötlejal vähemalt enne suuremahulist eriliiki isikuandmete ülekandmist üle kontrollida, kas vastutav töötleja suudab tuvastada taotluse esitanud isiku.[85]

Eraldi tähelepanuväärt on siinkohal esimeses lõigus välja toodud juhtmõte, et üldmääruse regulatsioonis tuleb viia identiteedivarguste risk miinimumi.[86] EL seadusandja ei ole selle eesmärgi täitmisel olnud kuigivõrd edukas, sest üldmääruse regulatsioonist ei tulene vastutava töötleja otsest ja sõnaselget kohustust tuvastada andmete ülekandmise taotluse esitanud isiku identiteeti. Positiivne on siiski, et vastutavale töötlejale on artikli 12 lg-s 2 tagatud õigus keelduda andmete ülekandmise õiguse teostamisest, kui taotluse esitanud isikut ei ole võimalik tuvastada. Nimetatud sättele tuginedes tuleks tunnustada vastutava töötleja kohustust tuvastada taotluse esitanud andmesubjekt.

[85] P. Swire, Y. Lagos, lk 375.
[86] Vt viide 76.

2. KOLMANDATE ISIKUTE ÕIGUSTE RIIVE ANDMETE ÜLEKANDMISE ÕIGUSE TEOSTAMISEL

2.1. Andmete ülekandmise õiguse teostamisel potentsiaalselt riivatavad õigused

Üldmääruse artikkel 20 lg 4 sätestab, et lõikes 1 osutatud õigus ei kahjusta teiste isikute õigusi ja vabadusi. Isegi kui üldmääruse tekst keelab andmete ülekandmisel sõnaselgelt kolmandate isikute õiguste ja vabaduste kahjustamise (vt ka autori hinnangut üldmääruse artikli 20 lg 4 ebaõnnestunud tõlke kohta käesoleva magistritöö p-s 1.4.5), on ikkagi võimalik, et andmete ülekandmise õiguste teostamisel leiab aset kolmandate isikute õiguste ja vabaduste riive. Selgitusena olgu välja toodud, et kuigi üldmääruse artikkel 20 lg 4 kasutab terminit „teiste isikute õigused ja vabadused", siis artikli 29 töörühma suunistes on samas kontekstis kasutatud terminit „kolmandate isikute õigused ja vabadused",[87] ning ka ingliskeelses õiguskirjanduses viidatakse kolmandate isikute privaatsusõigusele.[88] Sellest lähtuvalt kasutab autor alljärgnevalt samuti terminit „kolmas isik", mis tähistab isikut, kelle õigusi ja vabadusi võidakse andmete ülekandmise õiguse teostamisel riivata või kahjustada.

Käesolevas peatükis otsin vastust küsimusele, kuidas on tagatud, et andmete ülekandmise õiguse rakendamine ei riivaks kolmandate isikute õigust eraelu kaitsele ja isikuandmete kaitsele. Ühtlasi otsin teises peatükis kinnitust magistritöö esimesele hüpoteesile: andmete ülekandmise õiguse teostamine riivab kolmandate isikute eraelu puutumatuse ja isikuandmete kaitse õigust, kui andmete ülekandmise õiguse teostamisel kantakse uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed.

Autor on analüüsitavaks õiguseks valinud just õiguse eraelu puutumatuse kaitsele ja isikuandmete kaitsele. Ka õiguskirjanduses on tõstatatud küsimus sellest, kuidas õigus andmete ülekandmiseks seostub põhiõigusega eraelu puutumatuse kaitsele ja isikuandmete kaitsele ja mis on andmete ülekandmise õiguse kontrolli olemus, mida andmete ülekandmise õigus andmesubjektidele püüab tagada.[89] Analüüsitavad õigused on EL-s kaitstud mitmetasandiliselt. Nii on PS §-s 26 sätestatud eraelu puutumatuse kaitse tagatud ka harta artikli 7 ja EIÕK artikli 8 alusel. Samuti sätestab harta artikkel 8 ainsa põhiõiguste kataloogina eraldi isiku õiguse isikuandmete kaitsele.

[87] Näiteks on artikli 29 töörühm andmete ülekandmise õiguse suunistes märkinud: „Selline kahjustamine toimuks näiteks juhul, kui andmete edastamine ühelt vastutavalt töötlejalt teisele takistaks kolmandatel isikutel teostada andmesubjektidena oma isikuandmete kaitse üldmääruse kohaseid õigusi (nagu õigus saada teavet, õigus tutvuda andmetega jne)." – Artikli 29 töörühm, lk 11.
[88] A. D. Vanberg, M. B. Ünver, lk 3.
[89] I. Graef jt 2018, lk 1365.

Loomulikult võiks potentsiaalselt riivatavaid õigusi ette kujutada teisigi. Näiteks riivet kolmanda isiku sõna- ja teabevabadusele, mis kätkeb endas ka arvamusvabadust. Samuti riivet kolmanda isiku õigusele intellektuaalomandi kaitsele ja õigusele ettevõtlusvabadusele. Kuna andmete ülekandmise õigust nähakse edasiarendusena isikuandmetega tutvumise õigusest (üldmääruse artikkel 15), on ka andmete ülekandmise õiguse juures peetud asjakohaseks vaadata andmetega tutvumise õigust selgitavat põhjenduspunkti 63. Selles on esile toodud, et andmetega tutvumise õigus ei tohiks kahjustada teiste isikute õigusi ega vabadusi, sealhulgas ärisaladusi ega intellektuaalomandit ning eelkõige tarkvara kaitsvat autoriõigust.[90] Õiguskirjanduses on nimetatud õiguste riivet seostatud ka andmete ülekandmise õigusega.[91] Seepärast on välja toodud ärisaladuse ja intellektuaalomandi temaatika andmete ülekandmise õiguse vaatepunktist autori hinnangul tulevikus samuti analüüsimist väärt. Käesolev töö keskendub aga kolmanda isiku õigusele eraelu puutumatusele ja isikuandmete kaitsele, sest autori hinnangul võib andmete ülekandmise õiguse teostamine kõige lihtsamini ja sagedamini kaasa tuua kolmandate isikute isikuandmete ülekandmise uue vastutava töötleja juurde. Seetõttu on kohane selgitada, kuidas kolmandate isikute õiguseid sellisel juhul kaitstakse.

Andmete ülekandmise õigust teostades võidakse riivata kolmanda isiku õigust eraelu puutumatuse kaitsele ja isikuandmete kaitsele juhul, kui andmesubjekt taotleb selliste andmete ülekandmist, milles sisalduvad samaaegselt andmete ülekandmist taotlenud andmesubjekti ja ka kolmanda isiku isikuandmed. Näiteks on see olukord, kus andmesubjekt taotleb e-posti teenuses salvestatud sõprade, tuttavate või sugulaste kontaktandmete ülekandmist ning palub olemasoleval teenusepakkujal need edastada uuele teenusepakkujale, või soovib üle kanda maksetehingute ajalugu senisest pangast teise panka.[92] Samuti näiteks juhtum, kus andmesubjekt taotleb selliste sotsiaalmeedia postituste ülekandmist teise vastutava töötleja juurde, milles on võimalik tuvastada kolmas isik. See võib riivata kolmanda isiku õigust eraelu kaitsele ja isikuandmete kaitsele, mille sätestavad nii harta, EIÕK kui ka PS.

2.2.Õigus eraelu kaitsele ja isikuandmete kaitsele kehtivas õiguses

Euroopa Liidu põhiõiguste harta (edaspidi harta) kuulutati välja 07.12.2000. aastal Nizza tippkohtumisel Euroopa Parlamendi, Euroopa Nõukogu ja Euroopa Komisjoni poolt. 2000. aastal ei omanud harta kui deklaratsioon õiguslikult siduvat tähendust. Harta jõustati 01.12.2009. aastal koos Lissaboni lepingu[93] jõustumisega.[94] Alates 01.12.2009 on harta seega

[90] Üldmäärus, põhjenduspunkt 63.
[91] A. D. Vanberg, M. B. Ünver, lk 2.
[92] Andmekaitse inspektsioon. Isikuandmete töötleja üldjuhend 19.03.2019, lk 37.
[93] Lissaboni leping. – ELT 2007/C 306/01.
[94] P. K. Tupay, lk 231 ja seal viidatud teos (viide 47).

õiguslikult siduv. Kõrvutades hartat PS-i ja EIÕK-ga, on harta neist ainus, mis eristab isiku õigust eraelu kaitsele ja õigust isikuandmete kaitsele. Lisaks on harta ainus maailma tasemel konventsioon ehk õigusakt, milles õigus isikuandmete kaitsele on iseseisva põhiõigusena sätestatud.[95]

Harta artikkel 7 sätestab: *Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust.*

Harta artikkel 8 sätestab:

1. Igaühel on õigus oma isikuandmete kaitsele.

2. Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist.

3. Nende sätete täitmist kontrollib sõltumatu asutus.

Analüüsides teise isiku õigust eraelu ja isikuandmete kaitsele, on kohane hartast välja tuua nii artikkel 7 kui ka artikkel 8. Siiski ei ole üheselt selge see, kuivõrd harta artiklitega 7 ja 8 kaitstud õigused saab samastada.[96] EK ei ole samuti võtnud selget seisukohta artiklites 7 ja 8 sisalduvate õiguste eristamiseks. EK praktikat iseloomustab pigem nende õiguste ühendamine.[97] Näiteks otsuses *Euroopa Komisjon vs The Bavarian Lager Co. Ltd* leidis kohus, et eraelu puutumatuse ja isikupuutumatuse võimalikku kahjustamist tuleb alati hinnata kooskõlas isikuandmete kaitset käsitlevate liidu õigusaktidega.[98]

Mitmed autorid on õiguskirjanduses aga seisukohal, et õigus isikuandmete kaitsele, mis kätkeb endas mh õiglase töötlemise, nõusoleku, seaduspärasuse ja mittediskrimineerimise põhimõtet, väljub privaatsusõiguse tavapärasest kohaldamisalast,[99] kuid siiski ei eita nad mõlema õiguse tihedat seost.[100] Ka EK otsus *Volker und Markus Schecke GbR and Hartmut Eifert vs Land Hessen* toetab sellist lähenemist, leides et harta artiklis 8 sätestatud õigus isikuandmete kaitsele on tihedalt seotud harta artiklis 7 sätestatud õigusega eraelu puutumatusele.[101] EK on selgitanud, et esiteks puudutab harta artiklitega 7 ja 8 tunnustatud õigus eraelu puutumatusele isikuandmete töötlemisel igasugust teavet tuvastatud või tuvastatava füüsilise isiku kohta, ning

[95] P. K. Tupay, lk 231.
[96] P. K. Tupay, lk 232.
[97] O. Lynskey, lk 574.
[98] EKo C-28/08 P, *Euroopa Komisjon vs The Bavarian Lager Co. Ltd*, p 59.
[99] P. K. Tupay, lk 232 ja seal viidatud teosed (viide 57).
[100] P. K. Tupay, lk 232.
[101] EKo liidetud kohtuasjades C-92/09 ja C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert vs Land Hessen*, p 47.

teiseks, et piirangud, mida võib õiguspäraselt seada isikuandmete kaitse õigusele, vastavad piirangutele, mis on EIÕK artikli 8 raames lubatavad.[102]

Euroopa inimõiguste ja põhivabaduste konventsioon (edaspidi EIÕK), mis allkirjastati 04.11.1950 Roomas ning jõustus Eesti suhtes alates 16.04.1996,[103] ei sisalda otsesõnu õigust isikuandmete kaitsele, kuid sätestab eraelu puutumatuse kaitse artiklis 8. EIK praktikas on õigus eraelu puutumatuse kaitsele ühendatud isiku õigusega privaatsusele, ning EIK on andnud privaatsusele laia tõlgenduse, hõlmates ka õigust isikuandmete kaitsele.[104] EIÕK artikkel 8 sätestab:

1. Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning korrespondentsi saladust.

2. Võimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.

EIÕK artiklis 8 sisalduv õigus eraelu kaitsele on nn klassikaline privaatsusõigus. Privaatsusõiguse kohaldamisala on täidetud, kui esiteks esineb *prima facie* isiku huvi privaatsuse vastu ja teiseks sekkutakse sellesse huvisse.[105]

Sarnaselt EIÕK-ga, ei sisalda ka 28.06.1992. a vastu võetud ja 03.07.1992 jõustunud Eesti Vabariigi põhiseadus (edaspidi nimetatud PS)[106] eraldi sätet õigusest isikuandmete kaitsele. Siiski sätestab PS § 26 igaühe õiguse perekonna- ja eraelu puutumatusele. PS § 26 sätestab: *Igaühel on õigus perekonna- ja eraelu puutumatusele. Riigiasutused, kohalikud omavalitsused ja nende ametiisikud ei tohi kellegi perekonna- ega eraellu sekkuda muidu, kui seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks.* PS kommentaarides selgitatakse, et eraelu kaitse üheks oluliseks valdkonnaks on isikuandmete kaitse.[107]

Põhiseaduses sisalduv isiku õigus eraelu kaitsele on eriline selle poolest, et PS § 26 esemelise kaitseala sisustamisel tuleb arvestada, et PS-s on olemas üldisem säte, mis võib omada tähtsust

[102] EKo liidetud kohtuasjades C-92/09 ja C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert vs Land Hessen*, p 52.
[103] Inimõiguste ja põhivabaduste kaitse konventsioon [terviktekst]. – RT II 2000, 11, 57.
[104] EIKo 13710/88 *Niemietz vs Germany*, p-d 27-33.
[105] O. Lynskey, lk 583.
[106] Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
[107] Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne 2017. § 26/24. Kättesaadav veebis: https://www.pohiseadus.ee/

eraelu kaitsmisel. Selleks on PS § 19, mille lg 1 tagab õiguse vabale eneseteostusele.[108] PS § 19 lg 1 käsitatakse üldise vabaduspõhiõigusena, mis käsitleb õiguslikku vabadust teha ja jätta tegemata mida iganes. Lisaks sellele on leitud, et PS § 19 lg-s 1 on tagatud üldine isiksus- või isikupõhiõigus, mis kaitseb isiku puutumatust kui kitsamat isikusfääri ja selle säilimise õiguslikke põhitingimusi. Isikupõhiõiguse kaitse alla on arvatud enesemääramis- ja enesekujutamise õigus.[109] Riigikohus on käsitlenud enesemääramise ja enesekujutamise õigusega seotud olukordi sageli seoses PS § 19 lg-s 1 tagatud isiksuspõhiõigusega ja PS §-ga 26 tagatud eraelu puutumatusega.[110]

Analüüsi aluseks on seega harta artiklist 7 tulenev isiku õigus eraelu kaitsele, harta artiklist 8 tulenev isiku õigus isikuandmete kaitsele, EIÕK artiklist 8 tulenev isiku õigus eraelu kaitsele, PS §-st 19 tulenev õigus vabale eneseteostusele ja PS §-st 26 tulenev isiku õigus eraelu kaitsele.

2.3. Andmete ülekandmise õiguse teostamine langeb kolmanda isiku õiguse isikuandmete kaitsele ja eraelu kaitsele esemelisse kohaldamisalasse

EK on otsuses *Österreichischer Rundfunk* kujundanud metoodika, mida kasutatakse kaasuste lahendamisel, kus on üheaegselt võimalik isikuandmete kaitse õiguse riive kui ka privaatsusõiguse riive. Sellise integreeritud metoodika põhjenduseks on asjaolu, et EK ei ole oma praktikas eristanud isikuandmete kaitse õiguse ja eraelu puutumatuse õiguse kohaldamisala, vaid on need kaks õigust ühendanud. Kui andmesubjekt taotleb andmete ülekandmist ning vastavad andmed puudutavad samaaegselt ka kolmandat isikut ehk sisaldavad tema isikuandmeid, siis saab potentsiaalne riive kolmanda isiku õigusele isikuandmete kaitsele ja eraelu kaitsele esineda üksnes juhul, kui täidetud on esemelise kohaldamisala eeldused. Need on järgnevad: (i) tegemist on kolmanda isiku isikuandmetega üldmääruse artikli 4 p 1 mõttes; (ii) nende andmete kogumine ja kasutamine asjassepuutuva asutuse poolt ning nende edastamine kolmandale isikule on isikuandmete töötlemine üldmääruse artikli 4 p 2 mõttes; ja (iii) esineb isiku eraellu sekkumine.[111]

1. Tegemist on kolmanda isiku isikuandmetega üldmääruse artikli 4 p 1 mõttes.

Esimene kriteerium saab täidetud juhul, kui andmesubjekt soovib ühe teenusepakkuja juurest teise juurde üle kanda andmeid, mille abil on võimalik tuvastada lisaks andmesubjektile endale

[108] PõhiSK § 26/5.
[109] PõhiSK § 26/6 (viidatud: M. Ernits. Kommentaar PS §-le 19, p 3.1.2 (koos alapunktidega) väljaandes Ü. Madise jt. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Kolmas, täiendatud väljaanne. Tallinn: Juura, Õigusteabe AS, 2012. Sarnaselt R. Alexy. Põhiõigused Eesti põhiseaduses. Juridica 2001, lk 5-96, p 6.1).
[110] PõhiSK § 26/7.
[111] EKo liidetud kohtuasjades C-465/00, C-138/01 ja C-139/01, *Österreichischer Rundfunk*, p-d 64 ja 73.

ka kolmas isik ehk tegemist on samaaegselt kolmanda isiku isikuandmetega üldmääruse artikli 4 p 1 mõttes.

Ülekantavad andmed sisaldavad kolmanda isiku isikuandmeid, kui kolmas isik on neilt tuvastatud või otseselt või kaudselt tuvastatav üldmääruse artikli 4 p 1 mõttes.

2. Nende andmete kogumine ja kasutamine asjassepuutuva asutuse poolt ning nende edastamine kolmandale isikule on isikuandmete töötlemine üldmääruse artikli 4 p 2 mõttes.

Teine kriteerium eeldab, et riive kolmanda isiku õigustele ja vabadustele võib tekkida alles siis, kui teda puudutavaid isikuandmeid teise vastutava töötleja juures töödeldakse. Kriteeriumi järgi peab töötlemise näol olema tegemist andmete kogumise või kasutamisega või nende edastamisega kolmandale isikule üldmääruse artikli 4 p 2 mõttes. Andmete edastamine kolmandale isikule andmete ülekandmise õiguse vaatepunktist on andmete edastamine uuele vastutavale töötlejale. Ka see on käsitletav andmete töötlemisena artikli 4 p 2 mõttes.

Lisaks tuleb arvestada, et andmed ei tohi jääda andmesubjekti isiklikku kasutusse, sest üldmääruse artikkel 2 lg 2 p c sätestab, et üldmäärust ei kohaldata, kui isikuandmeid töötleb füüsiline isik eranditult isiklike või koduste tegevuste käigus. Seda kinnitab ka üldmääruse põhjenduspunkt 18, mille järgi ei tuleks kohaldada käesolevat määrust isikuandmete töötlemise suhtes, mida füüsiline isik teostab eranditult isiklikel või kodustel eesmärkidel ja seega väljaspool ametialast või äritegevust. Isiklik ja kodune tegevus võiks hõlmata kirjavahetust ja aadresside loetelu või tegevust suhtlusvõrgustikes ja internetis, mida tehakse sellise isikliku või koduse tegevuse raames.[112] Andmed jääksid andmesubjekti isiklikku kasutusse juhul, kui andmesubjekt soovib saada vastutavalt töötlejalt koopiat isikuandmetest, mida vastutav töötleja tema kohta hoiab ega kannaks isikuandmeid teise vastutava töötleja juurde üle. Sellisel juhul artikli 2 lg 2 p c alusel üldmääruse regulatsiooni tervikuna ei kohaldata.

Kui andmesubjekt kannab ise teise vastutava töötleja juurde üle isikuandmed, mis sisaldavad ka kolmanda isiku isikuandmeid, või nõuab taoliste isikuandmete ülekandmist otse ühelt vastutavalt töötlejalt teisele, siis toimub igal juhul isikuandmete töötlemine üldmääruse artikli 4 p 2 mõttes.

3. Esineb isiku eraellu sekkumine.

Kolmanda kriteeriumi kohaselt peab esinema isiku eraellu sekkumine.

[112] Üldmäärus, põhjenduspunkt 18.

EK on näiteks otsuses *Volker und Markus Schecke* leidnud, et harta artikli 7 mõttes on sekkumine isiku eraellu muuhulgas see, kui andmed avaldatakse veebisaidil ja andmed muutuvad kolmandatele isikutele kättesaadavaks.[113]

Samuti on EK näiteks otsuses *Österreichischer Rundfunk* leidnud, et kuigi oma töötajatele makstud palga kohta isikuandmete salvestamine tööandja poolt ei ole iseenesest eraellu sekkumine, riivab nende andmete edastamine kolmandale isikule asjassepuutuvate isikute õigust eraelu puutumatusele. EK täpsustas samas lahendis veel, et riive isiku õigusele eraelu puutumatusele esineb hoolimata sellest, milleks edastatud teavet edaspidi kasutatakse, ning kujutab endast seega sekkumist EIÕK artikli 8 tähenduses.[114] Lahendis *Amann vs Sveitš* täpsustas EIK, et sellise sekkumise puhul ei ole oluline, kas edastatud isikuandmed on delikaatsed või mitte või kas asjassepuutuvad isikud on selle sekkumise tõttu pidanud taluma mingeid ebamugavusi.[115] Piisab sellest, et vastutav töötleja on edastanud andmed kolmandatele isikutele.[116] Lähtudes EK ja EIK kohtupraktikast, võib üldistavalt öelda, et teise isiku eraellu sekkumine esineb, kui tema isikuandmed edastatakse kolmandale isikule.

Samas on Euroopa Kohtus arutatud kaasuses *Bavarian Lager*, kas näiteks isiku nime avalikustamine tema kutsetegevuse raames on privaatsusesse sekkumine või mitte. Kohus leidis, et üldjuhul ei oma isiku nime avalikustamine kutsetegevuse kontekstis seost isiku eraeluga, ning sellisel puhul ei ole kaalul isiku huvi privaatsuse vastu.[117] Sellest järeldub, et mitte alati ei ole andmete edastamine kolmandale isikule käsitletav sekkumisena isiku eraellu, kui sellistel andmetel puudub otsene seos isiku eraeluga, mida harta artikli 8 ja EIÕK artikli 8 alusel kaitstakse.

Euroopa Kohtu otsustest *Volker und Markus Schecke*, *Österreichischer Rundfunk* ja *Bavarian Lager* võib üldistatult järeldada, et sekkumine isiku eraellu on tema isikuandmete avalikustamine kolmandale isikule, kui sellistel andmetel on seos isiku eraeluga. Küll aga ei saa kutsetegevusega tegutseva isiku nime avalikustamist pidada eraellu sekkumiseks, sest kutsetegevuses tegutsev isik peab arvestama, et sellega kaasneb tema nime avalikustamine, kasutamine jne. Vastasel juhul on tal kutsetegevusega tegelemine oluliselt takistatud. Isiku nime avalikustamine kutsetegevuse raames on tõenäoliselt enamikel juhtudel vältimatu ning seetõttu ei oma kutsetegevuses tegutseva isiku nimi eraldivõetuna tihedat seost isiku eraelu

[113] EKo liidetud kohtuasjades C-92/09 ja C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert vs Land Hessen*, p 58.
[114] EKo liidetud kohtuasjades C-465/00, C-138/01 ja C-139/01, *Österreichischer Rundfunk,* p 74.
[115] EIKo 27798/95, *Amann vs. Šveits*, p 70.
[116] EKo liidetud kohtuasjades C-465/00, C-138/01 ja C-139/01, *Österreichischer Rundfunk,* p 75.
[117] EKo C-28/08 P, *Euroopa Komisjon vs The Bavarian Lager Co. Ltd*, p 46.

puutumatusega. Samas omab aga isiku kutsetegevuses teenitud töötasu puutumust isiku eraeluga, sest töötasu kasutab ta mh ka eraelulistel eesmärkidel ning selle avalikustamise üle peaks jääma otsustusõigus isikule endale. Mis puudutab isiku teenitavat töötasu, siis ei saa sedasama põhimõtet üks-üheselt kohaldada ametnikele avalikus teenistuses, kes peavad arvestama mõnevõrra suurema isikuandmete avalikustatuse tasemega[118] kui töölepingulised töötajad eraettevõtetes.

Seega harta artikli 7 mõttes sekkutakse kolmanda isiku eraellu juhul, kui kolmanda isiku isikuandmed edastatakse uuele vastutavale töötlejale ning selliste isikuandmete edastamisel, avalikustamisel või mis tahes muul toimingul on seos kolmanda isiku eraeluga. Varasemalt toodud näites saavad e-posti teenuses salvestatud sõprade, tuttavate ja sugulaste kontaktandmete ülekandmisel uue vastutava töötleja juurde vastutavale töötlejale teatavaks nimetatud isikute isikuandmed. Sellised kolmandate isikute isikuandmed on näiteks isiku nimi, telefoninumber, e-posti aadress jm teave, mis ülekandmise korral vastutavale töötlejale avalikustatakse. Samuti võib ette kujutada olukorda, kus andmesubjekt taotleb selliste sotsiaalmeedia postituste ülekandmist teise vastutava töötleja juurde, milles on võimalik tuvastada kolmas isik. Postituste ülekandmisel avalikustatakse kolmanda isiku isikuandmed piiratud või piiramata isikute ringile. Mõlemas näites, nii e-posti teenuses salvestatud kontaktandmete kui sotsiaalmeedia postituste puhul, on tuvastatav kolmandate isikute isikuandmete avalikustamine piiratud või piiramata isikute ringile ja sellest tulenev seos nende isikute eraeluga.

Järelikult esineb isiku eraellu sekkumine juhul, kui teda puudutavad isikuandmed edastatakse kolmandale isikule ning selliste isikuandmete edastamisel, avalikustamisel või mis tahes muul toimingul on seos isiku eraeluga.

Samal ajal on andmete ülekandmise puhul tegemist ka isikuandmete töötlemisega, mis kuulub harta artikli 8 lg 2 kohaldamisalasse, sest on täidetud kaks kriteeriumi: tegemist on isikuandmetega ja isikuandmeid töödeldakse. Andmete ülekandmine kui toiming on juba iseenesest käsitletav üldmääruse artikli 4 p 2 kohase isikuandmete töötlemisena, sest ülekandmine on automatiseeritud toiming, mille käigus isikuandmeid edastatakse ja/või avalikustatakse andmesubjektile endale või teisele vastutavale töötlejale. Ilma andmete edastamiseta või avalikustamiseta andmesubjektile või teisele vastutavale töötlejale kui

[118] Avaliku teenistuse seaduse § 65 lg 1 kohaselt avalikustatakse ametniku põhipalk jooksva kalendriaasta seisuga avalikustatakse avaliku teenistuse kesksel veebilehel hiljemalt 1. mail. Sama sätte lg 2 näeb ette, et ametniku põhipalk ja muutuvpalk ning tema teenistusülesannetest tulenev muu tulu kogusummana eelmise kalendriaasta kohta avalikustatakse avaliku teenistuse kesksel veebilehel hiljemalt 1. mail. – Avaliku teenistuse seadus. – RT I, 13.03.2019, 37.

isikuandmete töötlemise toiminguta ei saa andmete ülekandmise õigust teostada. Kuivõrd andmete ülekandmise õiguse kohaldamisalasse kuuluvad ainult isikuandmed üldmääruse artikli 4 p 1 mõttes, siis saab väita, et andmete ülekandmise õiguse teostamine on igal juhul ja alati isikuandmete töötlemine üldmääruse artikli 4 p 2 tähenduses. Seetõttu kuulub andmete ülekandmise õiguse teostamine harta artikli 8 kohaldamisalasse.

EIÕK artikkel 8 sätestab mh ka isiku õiguse eraelu kaitsele. EIK on selgitanud, et mõistet „eraelu" ei tuleks tõlgendada kitsalt.[119] EIK on otsuses *S. ja Marper vs Ühendkuningriik* kokkuvõtlikult selgitanud, kuidas EIK on seni sisustanud isiku õigust eraelu puutumatusele. EIK hinnangul on isiku eraelu on lai mõiste, millele ei saa anda ammendavat definitsiooni. See hõlmab mitmeid aspekte isiku füüsilisest ja psühholoogilisest puutumatusest, nt sooline enesemääramine, nimi ja seksuaalne sättumus, seksuaalelu. Lisaks on hõlmatud isiku perekonnaga seonduv teave, isiku tervisega seonduv teave, samuti nt rahvuslik kuuluvus ja rassiline päritolu. Muu hulgas kaitseb õigus eraelu puutumatusele ka isiku õigust suhelda välismaailmaga ja luua suhteid teiste isikutega. Samuti on ka kaitstud isiku õigus enda kuvandi loomisele. Sellest lahendist nähtuvalt pidas kohus isiku eraellu sekkumiseks ainuüksi isiku eraelu puudutavate andmete säilitamist ning märkis, et kui kohus hindab, kas konkreetsed isikuandmed seonduvad isiku eraeluga, tuleb arvesse võtta andmete salvestamise ja säilitamise konteksti, salvestatud andmete olemust ja viisi, kuidas salvestatud andmeid kasutatakse ja töödeldakse.[120]

Eeltoodud näidete puhul (e-posti teenuses salvestatud kontaktid või sotsiaalmeedia postitused) saab kergesti jaatada teise isiku eraellu sekkumist, arvestades laia tõlgendust, mida EIK eelistab EIÕK artikli 8 tõlgendamisel. E-posti teenuses salvestatud sõprade, tuttavate ja sugulaste kontaktandmete ülekandmisel uue vastutava töötleja juurde edastatakse teisele vastutavale töötlejale kolmandaid isikuid puudutavad andmed, nt nimi, telefoninumber, e-maili aadress. See on käsitletav sekkumisena kolmanda isiku eraellu. Sama kehtib ka teise näite puhul: kui andmesubjekt kannab teise vastutava töötleja juurde üle sotsiaalmeedia postitused, millelt on võimalik tuvastada ka kolmas isik, muutuvad kolmanda isiku isikuandmed kättesaadavaks piiratud või piiramata isikute ringile. Ka selle näite puhul sekkutakse kolmanda isiku eraellu, sest teda puudutavad isikuandmed avalikustatakse piiratud või piiramata isikute ringile, kelle valimist kolmas isik ei saa mõjutada.

[119] EIKo 27798/95, *Amann vs. Šveits*, p 65.
[120] Autori tõlge eesti keelde. EIKo 30562/04 ja 30566/04, *S. ja Marper vs. Ühendkuningriik*, p 67.

Eraellu sekkumine on käsitletav ka sekkumisena PS §-s 26 sätestatud õigusesse era- ja perekonnaelu kaitsele. PS kommentaarides on selgitatud, milline on PS § 26 esemeline kaitseala võrreldes EIÕK artikli 8 kaitsealaga: „Ka laialt tõlgendades on § 26 esemeline kaitseala kitsam EIÕK art 8 lg-s 1 sätestatust, kuna mõned era- ja perekonnaelu tahud, mis kuuluvad EIÕK art 8 kaitsealasse, on PS-s kaitstud spetsiifiliste põhiõigustega. Au ja head nime kaitseb § 17, kodu puutumatust § 33, sõnumite saladust § 43. Perekonna- ja eraelu üksikud tahud võivad kuuluda ka §-des 27 ja 42, samuti § 44 lg-s 2 sõnastatud põhiõiguste kaitsealasse. PS § 26 kui üldsätet tuleb kohaldada juhul, kui kaitsmist vajav erasfääri kuuluv hüve ei ole PS-s kaitstud mõne erisättega. Kui erisäte on olemas, tuleb kohaldada vastavat erisätet ja § 26 kui üldisem säte peab taanduma.“[121]

PS ei sisalda erisätet isiku eraellu sekkumise kaitseks või isikuandmete kaitseks, mistõttu tuleb kohaldada PS § 26 või PS § 19. Riigikohus on haldusasjas, kus kaebaja esitas nõude tunnistada süüdistavate hinnangute avaldamine õigusvastaseks, PS § 26 osas selgitanud: „Eraelu kaitse üheks oluliseks valdkonnaks on isikuandmete kaitse. Eraelu puutumatuse riivena käsitatakse muu hulgas isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist. Tulenevalt IKS § 4 lg-st 1 on isikuandmed mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on.“[122] Riigikohus on seega andmete avalikustamise kontekstis pidanud asjakohaseks PS § 26 kohaldamist.

Lisaks on PS kommentaarides selgitatud, et „[a]rvestades PS § 26 sõnastuslikku sarnasust EIÕK art-ga 8, oleks aga põhjendatud sisustada PS § 26 pigem avara kaitsealaga eraelu garantiina, mis hõlmab ka seni PS § 19 lg-st 1 tuletatud isiksuspõhiõiguse kaitsevaldkonnad (eelkõige enesemääramis- ja enesekujutamise õigus). Sellist lähenemist toetab ka Riigikohtu tõdemus, et esemeliselt kaitseb PS § 26 kõiki eraelu valdkondi, mis ei ole kaitstud eriõigustega (RKPJKo 25.06.2009, 3-4-1-3-09, p 16).“[123]

Kuivõrd PS ei sätesta isikuandmete kaitset puudutavaid eriõigusi ega –vabadusi, on kohane lähtuda PS §-st 26. Sisustades PS § 26 kohaldamisala, saab jõuda samale tulemusele nagu sisustades EIÕK artikli 8 kohaldamisala, sest PS § 26 puhul tunnustatakse EIÕK artikli 8 eeskujuks võtmist. EIK toetab EIÕK artikli 8 laia tõlgendamist[124] ning seetõttu tuleks ka PS § 26 kohaldamisala laialt tõlgendada. PS § 26 kohast eraellu sekkumist välja toodud näidete puhul tuleb seega jaatada, samuti nagu EIÕK artikli 8 puhul: e-posti teenuses salvestatud

[121] PõhiSK § 26/14.
[122] RKHKo 3-3-1-3-12, p 19.
[123] PõhiSK § 26/8.
[124] EIKo 27798/95, *Amann vs. Šveits*, p 65.

kontaktandmete ülekandmisel avalikustatakse kolmandat isikut puudutavad isikuandmed vastutavale töötlejale ning sotsiaalmeedia postituste ülekandmisel avalikustatakse kolmanda isiku isikuandmed piiratud või piiramata isikute ringile, seega sekkutakse kolmanda isiku eraelu sfääri.

2.4.Riive kolmanda isiku õigusele isikuandmete kaitsele ja eraelu puutumatusele

Väljakujunenud EK praktikast tulenevalt ei ole põhiõigused absoluutsed õigused, vaid neile võib seada piiranguid tingimusel, et need piirangud vastavad tegelikult meetmega taotletud üldise huvi eesmärkidele ega kujuta endast taotletavat eesmärki arvestades ülemäärast ja lubamatut sekkumist, mis kahjustaks tagatud õiguste sisu.[125] Seega on kohtupraktikas tunnustatud lähenemine see, et kui põhiõigus ei ole absoluutne õigus, võib seda piirata üksnes juhul, kui see on seadusega lubatud ega kahjusta ülemääraselt kõnealust põhiõigust. Vastuoludele põhiõiguste vahel tuleb läheneda kaasusepõhiselt ja kaaluda omavahel vastanduvaid põhiõiguseid ja nende võimalikku piiramist. Ka harta artikli 52 kohaselt tohib hartaga tunnustatud õiguste ja vabaduste teostamist piirata ainult seadusega ning arvestades nimetatud õiguste ja vabaduste olemust. Proportsionaalsuse põhimõtte kohaselt võib piiranguid seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi.

Järgnevalt analüüsin võimalikku õiguste riivet Euroopa Kohtu praktikas[126] välja kujundatud põhiõiguste võimaliku riive õiguspärasuse kriteeriumide alusel:

1. Piirang on seadusega ette nähtud;
2. Piirang järgib ühte või mitut legitiimset eesmärki;
3. Piirang on selle eesmärgi või nende eesmärkide saavutamiseks demokraatlikus ühiskonnas vajalik.[127]

Võrdluse korras olgu märgitud, et Euroopa Inimõiguste Kohus on EIÕK artiklit 8 puudutavas kaasuses lähtunud neljaastmelisest analüüsist: (i) esineb sekkumine isiku eraellu; (ii) sekkumine on seadusega kooskõlas; (iii) sekkumisel oli üks või mitu legitiimset eesmärki; (iv) sekkumine oli demokraatlikus ühiskonnas vajalik.[128] Võrreldes EK kasutatava skeemiga, on põhielemendid samad, kuid EIK on eraldi välja toonud isiku eraellu sekkumise kriteeriumi. Seda on magistritöös analüüsitud esemelise kohaldamisala juures peatükis 2.3.

[125] EKo C-418/11, *Texdata Software*, p 84, tsiteerides EKo C-28/05, *Dokter*, p 75 ja ühendatud kohtuasju EKo C-317/08 ja C-320/08, *Alassini* p 63.
[126] EKo liidetud kohtuasjades C-465/00, C-138/01 ja C-139/01, *Österreichischer Rundfunk.*
[127] EKo liidetud kohtuasjades C-465/00, C-138/01 ja C-139/01, *Österreichischer Rundfunk*, p 76.
[128] EIKo 13710/88, *Niemietz vs Germany*, p-d 27-37.

Kuivõrd EK ei ole eristanud harta artiklite 7 ja 8 kohaldamist isikuandmete kaitse vaidlustes,[129] siis analüüsib ka autor käesolevaga üheaegselt riivet teise isiku õigusele isikuandmete kaitsele ja eraelu puutumatusele.

1. Andmete ülekandmise õigus on seadusega ette nähtud.

Üldmääruse artikkel 20 lg 1 sätestab, et andmesubjektil on õigus saada teda puudutavaid isikuandmeid, mida ta on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul ning õigus edastada need andmed teisele vastutavale töötlejale, ilma et vastutav töötleja, kellele kõnealused isikuandmed on esitatud, seda takistaks, kui a) töötlemine põhineb artikli 6 lõike 1 punktis a või artikli 9 lõike 2 punktis a osutatud nõusolekul või artikli 6 lõike 1 punktis b osutatud lepingul ning b) töödeldakse automatiseeritult.

Nimetatud säte annab andmesubjektile õiguse kanda teda puudutavad isikuandmed üle teise vastutava töötleja juurde, kuid võib juhtuda, et andmete ülekandmisel kantakse üle ka kolmanda isiku isikuandmed. Sellisel juhul võivad jääda kolmanda isiku isikuandmed kaitseta. Seepärast tuleb hinnata, kas andmete ülekandmise õiguse teostamine riivab teise isiku õigust eraelu puutumatusele ja isikuandmete kaitsele. Andmete ülekandmise õigus on seega seadusega ettenähtud piiranguks kolmanda isiku õigusele eraelu puutumatuse kaitsele ja isikuandmete kaitsele.

Euroopa Kohtu praktikas on seadusega ette nähtud piirangu olemasolul peetud vajalikuks kontrollida, kas see kolmanda isiku õigusi piirav paragrahv on sätestatud piisavalt täpselt, et seaduse adressaatidel oleks võimalik oma käitumises sellest juhinduda, ning vastab seega Euroopa Inimõiguste Kohtu praktikas välja arendatud ootuspärasuse nõudele.[130] Eelnevalt mainitud ootuspärasuse nõue tähendab, et säte ei ole käsitletav seadusena, kui see ei ole formuleeritud piisavalt selgelt, et isik saaks oma käitumist juhtida. Isik peab olema võimeline, vajadusel asjakohase abiga, mõistlikus ulatuses ette nägema, millised tagajärjed tema käitumine kaasa toob. Need tagajärjed ei pea olema täieliku kindlusega ettenähtavad, sest kogemus näitab, et see on võimatu.[131]

Üldmääruse artikli 20 lg-test 1-2 tuleneb andmesubjektile õigus nõuda vastutavalt töötlejalt andmete ülekandmist. Nimetatud sätteid saab pidada piisavalt õigusselgeks vähemalt osas, mis sätestab andmesubjekti õiguse ülekandmist nõuda. Eelnevalt mainitud ootuspärasuse nõuet

[129] Vt viide 101.
[130] EKo liidetud kohtuasjades C-465/00, C-138/01 ja C-139/01, *Österreichischer Rundfunk*, p 77.
[131] EIKo 25390/94, *Rekvényi vs. Ungari*, p 34.

aitab üksikisiku vaatepunktist tagada ka see, et üldmääruse artikkel 20 ei anna liikmesriikidele võimalust andmete ülekandmise õiguse osas üldmäärusega ettenähtust kõrvale kalduda, st liikmesriikidel puudub kaalutlusõigus, kuidas andmete ülekandmise õigust teostada. Seega on potentsiaalselt kolmanda isiku õigusi piirav säte andmesubjekti seisukohast hinnatuna piisavalt täpse sõnastusega.

2. Andmete ülekandmise õigus järgib ühte või mitut legitiimset eesmärki.

Andmete ülekandmise õigusel on, nagu selgitatud käesoleva magistritöö peatükis 1.3, nii isikuandmete kaitse eesmärgid kui ka majanduslikud eesmärgid. Lühidalt öeldes on andmete ülekandmise õiguse põhiline eesmärk tagada andmesubjektile suurem kontroll teda puudutavate andmete üle (isikuandmete kaitse eesmärk). Lisaks kannab andmete ülekandmise õigus eesmärki vältida andmesubjekti „kinnijäämist" ühe teenusepakkuja juurde, ning toetada majanduslikku arengut (majanduslikud eesmärgid). Alljärgnevalt analüüsib autor, kas nendel eesmärkidel on kolmanda isiku õiguste eraelu kaitsele ja isikuandmete kaitsele piiramine õigustatud.

Eesmärk anda andmesubjektile suurem kontroll teda puudutavate isikuandmete üle tekitab olukorra, kus sisuliselt põrkuvad andmesubjekti õigus andmete ülekandmisele ja kolmanda isiku õigus eraelu kaitsele ja tema isikuandmete kaitsele. Seega tuleb otsida vastust sellele, kuidas ja mis ulatuses mõjutab andmete ülekandmine kolmanda isiku õigusi ning kas andmete ülekandmise õigus järgib legitiimset eesmärki.

Juhul kui ülekandmisel säilitatakse kolmanda isiku isikuandmete konfidentsiaalne tase, näiteks ülekantud e-kirju ei avaldata eelduslikult uue vastutava töötleja keskkonnas avalikkusele, vaid need jäävad ka edaspidi kahe isiku vaheliseks suhtluseks, ei saa pidada sekkumist kolmanda isiku eraellu kuigivõrd suureks. Siiski ei saa unustada, et nimetatud andmed saavad andmeid üle kandes teatavaks ka uuele vastutavale töötlejale. EK on leidnud, et ka nende andmete töötlemisega, mis avalikkusele kättesaadavad ei ole, kaasneb vältimatult see, et töötlemisest alates teab andmesubjekti eraelu puudutavat infot vastutav töötleja.[132] Kui aga ühest platvormist kantakse üle sotsiaalmeedia postitused, mis avaldatakse teise vastutava töötleja platvormil uuele jälgijaskonnale, on sekkumine kolmanda isiku eraellu tunduvalt suurem. Olenemata sellest, kas andmed avalikustatakse piiratud või piiramata isikute ringile, ei saa kolmas isik enda õiguste kaitseks määratleda ise isikute ringi, kellele nimetatud teave avalikustatakse. Sellisel juhul puudub kolmandal isikul võimalus kontrollida teda puudutavaid andmeid ning ta ei saa

[132] EKo ühendatud kohtuasjades C-468/10 ja C-469/10. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) vs. Administración del Estado*, p 45.

kaitsta oma isikuandmeid ja eraelu puutumatust. Seega on tuvastatud, et olenemata sellest, kui suures ulatuses kolmanda isiku isikuandmeid edastatakse või avalikustatakse (kas ainult uuele vastutavale töötlejale või piiratud või piiramata isikute ringile), sekkutakse vähemal või suuremal määral kolmanda isiku eraellu. Andmete ülekandmise õiguse eesmärk anda andmesubjektile suurem kontroll teda puudutavate isikuandmete üle toob järelikult kaasa sekkumise kolmanda isiku õigusesse eraelu kaitsele ja isikuandmete kaitsele. Olen seisukohal, et ainuüksi eesmärk anda andmesubjektile suurem kontroll teda puudutavate andmete üle ei peaks automaatselt tähendama, et andmesubjekti õigused on kaalukamad kui kolmandate isikute õigused. Võrdses olukorras ei peaks ühe isiku õigused olema ülemuslikud kolmanda isiku õiguste ees, vaid mõlemale isikule tuleks tagada võrdne õiguste kaitstuse tase.

Võimalik on, et kolmandat isikut puudutavad isikuandmed võisid juba enne andmete ülekandmist olla kas piiratud või piiramata isikute ringile avalikustatud. Andmete ülekandmisel toimub aga selliste isikuandmete täiendav avalikustamine. Riigikohus on haldusasjas 3-3-1-3-12 leidnud, et täiendaval avalikustamisel võivad olla kolmanda isiku jaoks olulised tagajärjed: „[a]inuüksi sellest, et andmed on isiku nõusolul või seaduse alusel ilma tema nõusolekuta varem mingis vormis avalikustatud, ei saa järeldada, et täiendaval avalikustamisel ei pruugi andmesubjekti jaoks olla olulisi tagajärgi. Andmete esialgne ja korduv avalikustamine võivad toimuda väga erinevas vormis ja väga erineva intensiivsusega, sõltuvalt andmete edastaja isikust, infokanalist, kontekstist, auditooriumist jne.“[133] Eeltoodu tähendab ühtlasi, et isegi kui kolmandat isikut puudutavad andmed olid kas piiratud või piiramata isikute ringile varasemalt avalikustatud, allub sellele vaatamata iga järgnev toiming kolmandat isikut puudutavate isikuandmetega isikuandmete kaitse üldmääruse regulatsioonile. Ka varem avalikustatud andmete edasine töötlemine on käsitletav isikuandmete töötlemisena üldmääruse artikli 4 p 2 mõttes.

Riigikohtu seisukohta haldusasjas 3-3-1-3-12 saab andmete ülekandmise õiguse vaatepunktist pidada eriti oluliseks. Nimelt kui kolmas isik kaotab kontrolli teda puudutavate isikuandmete üle ning need avalikustatakse tema teadmata piiratud või piiramata isikute ringile, võib see kolmanda isiku jaoks kaasa tuua olulised tagajärjed. Isegi kui kolmandat isikut puudutavad isikuandmed on juba varem kord avalikustatud, ei tähenda see, et selliste andmete mujal avaldamine ei sekkuks kolmanda isiku eraellu. Vastupidi, kolmanda isiku õigustesse sekkumisel ei tohiks osutuda määravaks see, kas andmeid saatva vastutava töötleja juures olid andmed avalikkusele kättesaadavad. Siinkohal tuleb arvestada, nagu ka ülal käsitletud, et

[133] RKHKo 3-3-1-3-12, p 24.

andmete ülekandmisel võib muutuda isikute ring, kellele andmed kättesaadavaks saavad. Isegi kui andmed olid ka varem teatud isikute ringile avalikult kättesaadavad, kuid andmete ülekandmisel andmetele ligipääsevate isikute ring muutub, võib andmete ülekandmise teostamine sekkuda kolmanda isiku eraellu ja tuua tema jaoks kaasa olulised tagajärjed.

Eeltoodut kokkuvõttes asub autor seisukohale, et andmete ülekandmise eesmärk anda andmesubjektile suurem kontroll teda puudutavate isikuandmete üle on iseenesest legitiimne eesmärk, kuid andmete ülekandmise õigust teostades (juhul, kui selle raames kantakse üle kolmanda isiku isikuandmed) sekkutakse alati vähemal või suuremal määral kolmanda isiku õigusesse eraelu kaitsele ja isikuandmete kaitsele. Isegi juhul, kui andmed on varasemalt avalikustatud, võib täiendav avalikustamine kaasa tuua kolmanda isiku jaoks olulised tagajärjed, sest teda puudutavad isikuandmed avalikustatakse ilma tema teadmata. Seepärast on sekkumine eriti tõsine juhul, kui kolmandat isikut puudutavad isikuandmed avaldatakse ilma kolmanda isiku kontrolli teostamise võimaluseta määratud või määratlemata isikute ringile.

Andmete ülekandmise õiguse eesmärki edendada majanduslikku arengut võib näha EL poolt tunnustatud üldist huvi pakkuva eesmärgina. Üldist huvi pakkuva eesmärgi näitena saab tuua EK otsuse kohtuasjas *Volker und Markus Schecke.* Kohus leidis, et õigusnorm, mis kohustab avaldama põllumajandustoetuse saajate nimed, aitab tugevdada avalikkuse kontrolli põllumajandustoetusteks makstud summade üle ning suurendab põllumajandustoetuste fondide kasutamise läbipaistvust.[134] Seeläbi edendatakse nendega EK hinnangul liidu poolt tunnustatud üldist huvi pakkuvat eesmärki.

Andmete ülekandmise õiguse puhul on artikli 29 töörühm on välja toonud, et kuna andmete ülekandmise õigus võimaldab edastada isikuandmeid otse ühelt vastutavalt töötlejalt teisele, on see ka oluline vahend, mis toetab isikuandmete vaba liikumist ELis ja soodustab vastutavate töötlejate vahelist konkurentsi.“[135] Sarnaselt EK otsuses *Volker und Markus Schecke* kohtuasjas tuvastatud üldist huvi pakkuva eesmärgiga, on ka andmete ülekandmise õiguse eesmärgid – vaba liikumine EL-is, vastutavate töötlejate vaheline konkurents – vaadeldavad üldist huvi pakkuvate eesmärkidena.

Seesama üldist huvi pakkuv majanduslik eesmärk on seostatav digitaalse ühisturu kontseptsiooniga EL-s. Digitaalse ühisturu loomisel on andmekaitse reform võtmetähtsusega teguriks. Euroopa Komisjon on seadnud digitaalse ühisturu prioriteetseks ning soovib seeläbi

[134] EKo liidetud kohtuasjades C-92/09 ja C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert vs Land Hessen*, p 67.
[135] Artikli 29 töörühm, lk 3.

anda Euroopa kodanikele ja ettevõtetele võimaluse digitaalmajandusest kasu saada.[136] Digitaalne ühisturg põhineb kolmel sambal: (1) parem juurdepääs internetis pakutavatele kaupadele ja teenustele, (2) digitaalvõrkude ja -teenuste arenguks sobivate tingimuste loomine ning (3) Euroopa digitaalmajanduse kasvupotentsiaal.[137] Andmete ülekandmise õiguse eesmärgil edendada majanduslikku arengut on seega ka laiemapõhjaline tähendus digitaalse ühisturu loomise kontekstis, mis annab kinnitust, et see on liidu poolt tunnustatud üldist huvi pakkuvaks eesmärgiks.

Siiski tekib küsimus, kas selline liidu poolt tunnustatud üldist huvi pakkuv majanduslik eesmärk on ka legitiimne eesmärk kolmanda isiku õigusesse eraelu kaitsele ja isikuandmete kaitsele sekkumisel. Autori arvates ei saa majanduslikku edu põhimõtteliselt seada kõrgemale isikute õiguste ja vabaduste kaitsest. Selleks peab esinema piisavalt oluline põhjus. Kui lähtuda sellest, et andmete ülekandmise õigus ei riiva kolmandate isikute õigust eraelu kaitsele ja isikuandmete kaitsele, viiks see olukorrani, kus andmesubjekti taotlusel kantakse valimatult kantakse üle ka kolmandaid isikuid puudutavad isikuandmed, kui need ülekantavate andmete hulgas sisalduvad. Andmete ülekandmine toimuks ilma, et kolmandatel isikutel säiliks kontroll enda andmete üle. Majanduslike huvide prevaleerimine üksikisikute põhiõiguste ees peaks olema erandlik juhtum, mitte üldpõhimõte.

Digitaalse ühisturu kontekstis kannab andmete ülekandmise õigus eesmärki vältida andmesubjekti nn kinnijäämist ühe teenusepakkuja (vastutava töötleja) juurde. Kui andmesubjekti taotlusel kantakse teise vastutava töötleja juurde üle ka kolmanda isiku isikuandmed, jättes täielikult arvestamata kolmandate isikute õigused, ei saa pidada andmesubjekti vastutava töötleja juurde kinnijäämise vältimist andmete ülekandmise õiguse legitiimseks eesmärgiks. Andmesubjekti kinnijäämise vältimise eesmärk oleks legitiimne juhul, kui see arvestaks samaaegselt nii andmesubjekti kui ka kolmanda isiku õiguste ja vabadustega. Õiglane lahendus kolmandate isikute õiguste ja vabadustega arvestamiseks oleks see, kui üldmäärus sätestaks, kuidas saavad kolmandad isikud ülekantud andmete osas kontrolli teostada, kuid selline regulatsioon üldmääruses puudub. Üldmäärus piirdub artiklis 20 lg 4 sätestatuga, et andmete ülekandmise õigus ei tohi kahjustada teiste isikute õigusi ja vabadusi, kuid ei reguleeri, kuidas teiste isikute õigusi ja vabadusi tegelikult kahjustamise eest kaitstakse.

[136] European Commission. Special Eurobarometer 431 „Data Protection“. Publication: June 2015, lk 6.
[137] S. Engels, J. B. Nordemann. The Portability Regulation (Regulation (EU) 2017/1128): A Commentary on the Scope and Application. – Journal of Intellectual Property, Information Technology, and Electronic Commerce Law 2018/9, lk 179.

Eesmärk edendada EL majandust on küll üllas, kuid nähes andmete ülekandmise õigust kui paindumatut vahendit majanduse edendamiseks, võib see viia olukorrani, kus isikuandmed muutuvad produktiks, mida vastutavad töötlejad on kohustatud edasi levitama.[138] Seejuures ei austata kolmandate isikute õigusi ja vabadusi. See aga tekitab riski, et vastutavad töötlejad võivad isikuandmete kogumeid näha kui majanduslikku väärtust, mida omavahel edastades soovitakse või loodetakse teenida kasumit. See omakorda tekitab väärarusaama isikuandmete tegelikust väärtusest ja isikuandmete kaitse võidakse jätta majandusliku edu saavutamise nimel sootuks tahaplaanile. Seetõttu ei saa pidada andmete ülekandmise õiguse majanduslikku eesmärki legitiimseks eesmärgiks kolmandate isikute õiguste ja vabaduste piiramisel.

3. Andmete ülekandmise õigus on selle eesmärgi või nende eesmärkide saavutamiseks demokraatlikus ühiskonnas vajalik.

EL õiguse üldpõhimõtete hulka kuuluv proportsionaalsuse põhimõte nõuab, et EL õigusaktiga rakendatavad meetmed oleksid taotletava eesmärgi saavutamiseks sobivad ega läheks kaugemale sellest, mis on eesmärgi saavutamiseks vajalik.[139] EK on otsustanud, et isikuandmete kaitse erandite ja piirangute puhul tuleb piirduda rangelt vajalikuga.[140]

Eesmärk anda andmesubjektile suurem kontroll teda puudutavate isikuandmete üle ja vältida andmesubjekti kinnijäämist ühe teenusepakkuja juurde tuleb ühitada harta artiklites 7 ja 8 ette nähtud põhiõigustega.[141] Eelkõige tuleb hinnata, kas nimetatud eesmärgi täitmiseks leidub isikute õigust eraelu puutumatusele ja isikuandmete kaitsele vähem riivavaid viise. EK on *Volker und Markus Schecke* otsuses pidanud vähem riivavaks näiteks isikuandmete täieliku avaldamise asemel üksnes isikuandmete piiratud avaldamist sõltuvalt põllumajandustoetuse saamise ajavahemikust, toetuse sagedusest või liigist ja tähtsusest.[142]

Võttes lähtepunktiks andmete ülekandmise õiguse, mille põhiline eesmärk on anda andmesubjektile suurem kontroll teda puudutavate isikuandmete üle, tuleb kindlaks teha, kas andmete ülekandmise õigust saaks teostada viisil, milles see riivaks vähem kolmandate isikute

[138] E. Pyykkö. Data protection at the cost of economic growth? – European Credit Research Institute Commentary 2012, No 11, lk 4. Kättesaadav veebis: https://www.ceps.eu/system/files/ECRI%20Commentary%20No%2011%20Data%20protection.pdf
[139] EKo C-58/08, *Vodafone jt*, p 51 ja seal viidatud kohtupraktika; EKo liidetud kohtuasjades C-92/09 ja C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert vs Land Hessen*, p 74.
[140] EKo C-73/07, *Satakunnan Markkinapörssi ja Satamedia*, p 56.
[141] EKo liidetud kohtuasjades C-92/09 ja C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert vs Land Hessen*, p 76.
[142] EKo liidetud kohtuasjades C-92/09 ja C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert vs Land Hessen*, p 81.

õigusi ja vabadusi. Vähem riivavaks saab pidada EK otsuse *Volker und Markus Schecke* põhjal näiteks isikuandmete täieliku avaldamise asemel isikuandmete avaldamise piiramist.

Toodud põhimõttest lähtumine ei ole aga andmete ülekandmise õiguse puhul tulemuslik, sest andmete ülekandmise õigus ei ole suunatud sellele, et vastutav töötleja kontrolliks iga andmesubjekti esitatud taotluse põhjal üksipulgi läbi andmesubjekti puudutavad isikuandmed ning üritaks nendest eraldada kolmandate isikute isikuandmeid. Andmete ülekandmise õigus on pigem vaadeldav automaatse ja tehnilise lahendusena, mis võimaldab andmete lihtsat ülekandmist. Et piirata kolmandat isikut puudutavate isikuandmete hulka ülekantavate andmete seas, peaks vastutav töötleja kõik ülekantavad andmed eraldi läbi töötama, kuid seda ei ole seadusandja andmete ülekandmise õiguse kehtestamisel artiklis 20 ette näinud.

Samas ei nähtu ka muid mõistlikke meetmeid, mida kasutades riivataks vähem kolmanda isiku õigust eraelu kaitsele ja isikuandmete kaitsele. Vähem riivavate meetmete puudumise tõttu tuleb asuda seisukohale, et andmete ülekandmise õigus on proportsionaalne andmete ülekandmise õiguse taotletava eesmärgiga anda andmesubjektile suurem kontroll teda puudutavate isikuandmete üle.

Kokkuvõtlikult olen seisukohal, et andmete ülekandmise õigus riivab kolmanda isiku õigust eraelu kaitsele ja isikuandmete kaitsele, sest andmete ülekandmise õiguse teostamisel kolmanda isiku isikuandmeid üle kandes sekkutakse alati vähemal või rohkemal määral kolmanda isiku eraellu. Andmete ülekandmise õiguse eesmärki edendada EL majandust ei saa pidada legitiimseks eesmärgiks kolmandate isikute õiguste eraelu kaitsele ja isikuandmete kaitsele piiramisel. Seetõttu leiab kinnitust magistritöö esimene hüpotees, et andmete ülekandmise õiguse teostamine riivab kolmandate isikute eraelu puutumatuse ja isikuandmete kaitse õigust, kui andmete ülekandmise õiguse teostamisel kantakse uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed.

3. KOLMANDATE ISIKUTE ÕIGUSTE JA VABADUSTE KAITSEKS ÜLDMÄÄRUSES ETTE NÄHTUD ABINÕUD

3.1. Andmete eraldatavuse võimalikkus kolmandate isikute õiguste ja vabaduste kaitse tagamiseks

Andmekaitse Inspektsioon (edaspidi AKI) on seisukohal, et kolmandate isikute õiguste rikkumise vältimiseks võib andmetöötleja andmekoosseise eelnevalt puhastada.[143] Artikli 29 töörühm on selgitanud, et andmete ülekantavus eeldab vastutavatelt töötlejatelt täiendavat andmetöötluse kihti, et andmeid platvormilt kätte saada ja eraldada ülekantavuse kohaldamisalast väljapoole jäävad isikuandmed, nagu kaudsed andmed või süsteemide turvalisusega seotud andmed. Sel viisil õhutatakse vastutavaid töötlejaid tegema oma süsteemides eelnevalt kindlaks need andmed, mis jäävad andmete ülekandmise õiguse kohaldamisalasse.[144]

AKI ja artikli 29 töörühm suunavad vastutavaid töötlejaid kolmandate isikute õiguste kaitseks andmetest eraldama kaudsed andmed või süsteemide turvalisusega seotud andmed. Artikli 29 töörühm on kaudsete või süsteemi loodud andmete all silmas pidanud vastutava töötleja poolt andmesubjekti esitatud andmete analüüsimise tulemusena loodud andmeid (vt lähemalt alapeatükk 1.4.4). Seepärast ei tuleks andmete eraldatavuse kriteeriumi all mõista vastutava töötleja poolt andmesubjekti puudutavate andmete läbitöötamist või sorteerimist, mille põhjal vastutav töötleja subjektiivselt otsustades valiks, kas teatud andmed üle kanda või mitte.

Sel põhjusel ei lahenda autori hinnangul andmete eraldatavuseks nn täiendava andmetöötluse kihi loomine kolmandate isikute õiguste ja vabaduste võimaliku riive esinemise probleemi. Artikli 29 alusel asutatud andmekaitse töörühm suunab vastutavaid töötlejaid eraldama täiendava andmetöötluse kihi abil kaudseid ja süsteemi loodud andmeid andmesubjekti poolt esitatud andmetest. Soovitatud andmete eraldamise teel ei saa aga eraldada kolmandate isikute isikuandmeid andmekogumist, sest kolmanda isiku isikuandmed ei ole „kaudsed“ või „süsteemi loodud“ andmed.

Seega tuleks andmete eraldatavuse kriteeriumi rakendamist vastutava töötleja poolt mõista eelkõige kui vastava tehnilise lahenduse loomist, mis võimaldab eraldada andmete ülekandmise õiguse kohaldamisalast väljapoole jäävad kaudsed andmed või süsteemi loodud andmed. Selle kaudu ei ole aga võimalik tagada kolmandate isikute õiguste ja vabaduste kaitset, kui ülekantavate andmete hulgas on ka kolmanda isiku isikuandmed.

[143] Andmekaitse Inspektsioon, lk 37.
[144] Artikli 29 töörühm, lk 18.

3.2.Andmete ülekandmise taotlusest keeldumine

Mitte alati ja eranditult ei pea vastutav töötleja täitma andmesubjekti esitatud taotlust andmesubjekti õiguste teostamiseks. Vastutava töötleja võimaluse andmesubjekti taotlusest keeldumiseks või taotluse eest mõistliku tasu küsimiseks sätestab üldmääruse artikkel 12 lg 5:

Artiklite 13 ja 14 kohase teabe esitamine ning artiklite 15–22 ja 34 kohane teavitamine ja meetmete võtmine on tasuta. Kui andmesubjekti taotlused on selgelt põhjendamatud või ülemäärased, eelkõige oma korduva iseloomu tõttu, võib vastutav töötleja kas:

a) küsida mõistlikku tasu, võttes arvesse halduskulu, mis kaasneb teabe esitamise või teavitamise või taotletud meetmete võtmisega, või

b) keelduda taotletud meetmete võtmisest.

Vastutaval töötlejal lasub kohustus tõendada, et taotlus on selgelt põhjendamatu või ülemäärane.

Autori eesmärk on käesolevas peatükis vastata järgmistele küsimustele: millal saab vastutav töötleja pidada andmesubjekti esitatud andmete ülekandmise taotlust selgelt põhjendamatuks või ülemääraseks? Millised võivad olla vastutava töötleja jaoks alused keeldumaks andmete ülekandmise taotluse rahuldamisest? Autor hindab, kas magistritöös seni analüüsitud turvarisk või riive kolmanda isiku õigusele eraelule ja isikuandmete kaitsele võivad olla andmete ülekandmise õiguse teostamisest keeldumise alused vastutava töötleja jaoks?

Vastutaval töötlejal on üldmääruse artikli 12 lg-st 5 tulenevalt õigus keelduda andmesubjekti esitatud taotluse täitmisest kui taotlus on selgelt põhjendamatu või ülemäärane. Nimetatud alused andmesubjekti taotlusest keeldumiseks on määratlemata õigusmõisted, mille sisustamine võib igal üksikjuhul sõltuda konkreetsetest asjaoludest. Näiteks tuleb arvestada andmesubjekti esitatud teisi taotlusi, vastutava töötleja poolt töödeldavate andmete vormingut vastutava töötleja juures, samuti ka nt seda, kas andmed on anonümiseeritud või pseudonümiseeritud jpm.

Artikli 29 töörühm on andmete ülekandmise õiguse juhendis vastutava töötleja keeldumise aluste kohta selgitanud: „Isikuandmete automatiseeritud töötlemisele spetsialiseerunud infoühiskonna teenuste puhul võib selliste automatiseeritud süsteemide nagu rakendusliideste kasutamine hõlbustada teabevahetust andmesubjektiga ja vähendada seega korduvatest taotlustest tingitud koormust. Seepärast peaks esinema väga vähe juhtumeid, kus vastutav

töötleja suudab põhjendada taotletud teabe esitamisest keeldumist, isegi mitme andmete ülekandmise taotluse puhul.“[145]

Õiguskirjanduses on veel selgitatud, et üldmääruse artikkel 12 lg 5 ei määra hierarhiat, kas vastutaval töötlejal tuleks eelistada andmesubjektilt mõistliku tasu küsimist või taotletud meetmete võtmisest keeldumist. Seega on vastutaval töötlejal diskretsiooniõigus artikli 12 lg-ga 5 kehtestatud keeldumise aluste vahel valimisel. Vastutaval töötlejal lasub kohustus tõendada, et taotlus on selgelt põhjendamatu või ülemäärane. Seepärast peaks vastutav töötleja korduvate taotluste puhul dokumenteerima saadud taotluste arvu, et olla võimeline täitma oma tõendamiskoormist ja tugineda andmesubjekti taotluste ülemäärasusele.[146] Selgelt põhjendamatud taotlused peaksid olema äärmiselt erandlikud, sest taotluse põhjendamatu iseloom peaks vastutavale töötlejale juba esmapilgul ilmnema.[147]

Selgelt põhjendamatu taotluse kohta saab tuua järgneva näite: isik taotleb vastutavalt töötlejalt üldmääruse artikli 15 alusel andmetega tutvumist, soovides saada teada, kas vastutav töötleja töötleb tema isikuandmeid või mitte. Vastutav töötleja kinnitab, et ei töötle tema isikuandmeid. Isik esitab sellele vaatamata samale vastutavale töötlejale taotluse andmete kustutamiseks üldmääruse artikli 17 alusel. Tema taotlus andmete kustutamiseks on selline, mida vastutav töötleja ilmselgelt ei ole võimeline teostama, sest vastutav töötleja ei töötle selle isiku isikuandmeid. Sellisel juhul on isiku esitatud taotlus „selgelt põhjendamatu“ üldmääruse artikli 12 lg 5 mõttes.[148]

Teine alus andmesubjekti esitatud taotlusest keeldumiseks või mõistliku tasu küsimiseks on see, et andmesubjekti esitatud taotlus on „ülemäärane, eelkõige oma korduva iseloomu tõttu“. Artikli 29 töörühm on seisukohal, et isegi mitme andmete ülekandmise taotluse puhul peaks esinema väga vähe juhtumeid, kus vastutav töötleja suudab põhjendada taotletud teabe esitamisest keeldumist.[149] Selline seisukoht on põhjendatud, sest andmete ülekandmise õiguste teostamisel eeldatakse vastutavalt töötlejalt sobivate tehniliste lahenduste olemasolu, kuivõrd üldmääruse artikli 20 lg 1 järgi on andmesubjektil õigus saada vastutavalt töötlejalt teda puudutavad andmed struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul. Sobivate tehniliste lahenduste olemasolul ei peaks andmesubjekti esitatud andmete

[145] Artikli 29 töörühm, lk 15.
[146] P. Voigt, A. von dem Bussche, lk 148 (viidatud: Kamlah, in: Plath, BDSG/DSGVO, Art. 12 (2016), rec. 20).
[147] P. Voigt, A. von dem Bussche, lk 148.
[148] P. Voigt, A. von dem Bussche, lk 148 (viidatud: Example drawn from Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 21).
[149] Artikli 29 töörühm, lk 15.

ülekandmise taotlused olema vastutava töötleja jaoks ülemäärased, isegi kui andmesubjekt neid korduvalt esitab.

Ühest küljest soodustavad sobivad tehnilised lahendused korduvalt esitatud andmete ülekandmise taotluste täitmist, kuid teisest küljest tuleb arvestada, et tõenäoliselt on vastutaval töötlejal kindlad vormingud, milles ta andmeid üle kanda saab. Kui andmesubjekt taotleb andmete ülekandmist mõnes vastutavale töötlejale ebasobivas vormingus, näiteks ei ole sellises vormingus andmete ülekandmine tehniliselt teostatav, võiks vastutav töötleja keelduda andmesubjekti esitatud taotluse täitmisest, tuginedes taotluse ülemäärasusele.

Seega selgub, millal saab vastutav töötleja pidada andmesubjekti esitatud andmete ülekandmise taotlust selgelt põhjendamatuks või ülemääraseks. Andmesubjekti esitatud andmete ülekandmise taotlust saab pidada selgelt põhjendamatuks, kui vastutaval töötlejal on objektiivselt võimatu andmesubjekti taotlust täita. Andmesubjekti esitatud taotlust andmete ülekandmiseks saab pidada ülemääraseks, eelkõige oma korduva iseloomu tõttu üksnes erandlikel juhtudel. Üldmäärusega eeldatakse vastutavalt töötlejalt sobivate tehniliste lahenduste kasutuselevõtmist, mis võimaldavad andmete ülekandmist struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul. Sobivate tehniliste lahenduste olemasolul ei peaks andmesubjekti korduvad taotlused andmete ülekandmiseks olema vastutava töötleja jaoks ülemäärased. Samas võib vastutava töötleja jaoks olla andmete ülekandmise taotlusest keeldumise aluseks taotluse ülemäärasus, kui andmesubjekt taotleb andmete ülekandmist mõnes vastutava töötleja tehnilistele lahendustele mittevastavas vormingus.

Lisaks annan hinnangu, kas magistritöös seni analüüsitud riive kolmanda isiku õigusele eraelule ja isikuandmete kaitsele võib olla andmete ülekandmise õiguse teostamisest keeldumise aluseks vastutava töötleja jaoks. Seejärel selgub, kas leiab kinnitust magistritöös püstitatud teine hüpotees: vastutaval töötlejal ei ole võimalik keelduda kolmanda isiku õiguste ja vabaduste kaitse põhjendusel andmesubjekti esitatud andmete ülekandmise taotluse täitmisest.

Andmete ülekandmise taotluse saamisel ei tule artikli 29 töörühma hinnangul vastutaval töötlejal andmesubjekti puudutavaid andmeid läbi töötada või sorteerida. Soovituslik on luua täiendav andmekaitse kiht, mille abil eraldatakse andmesubjekti puudutavast andmekogumist kaudsed või süsteemi loodud andmed, mis andmete ülekandmise õiguse kohaldamisalasse ei kuulu (vt selle kohta ka käesoleva töö alapeatükk 3.1).[150] Ka üldmääruse tekst ei kohusta vastutavat töötlejat ülekantavaid andmesubjekti puudutavaid andmeid läbi vaatama või nendega sisuliselt tutvuma. Sellest nähtuvalt toimub andmete ülekandmine ilma vastutava töötleja poolt

[150] Vt viide 144.

andmesubjekti puudutavaid andmeid läbi töötamata ja nendega sisuliselt tutvumata. Seetõttu ei saa vastutav töötleja aga teadlikuks sellest, kas andmete hulgas sisaldub kolmandaid isikuid puudutavaid isikuandmeid.

Juhul, kui andmete ülekandmise käigus kantakse ühes andmesubjekti andmetega uue vastutava töötleja juurde ka kolmanda isiku isikuandmed, ei saa vastutav töötleja kolmanda isiku isikuandmete ülekandmisest isegi teadlikuks. Seepärast jääb alles risk, et kolmandat isikut puudutavad isikuandmed kantakse teise vastutava töötleja juurde andmete ülekandmise õiguse alusel üle ning esineb riive kolmanda isiku õigusele eraelu kaitsele ja isikuandmete kaitsele. Vastutaval töötlejal ei ole võimalik keelduda kolmanda isiku õiguste ja vabaduste kaitse põhjendusel andmesubjekti esitatud andmete ülekandmise taotluse täitmisest, sest vastutav töötleja ei saa andmekogumis sisalduvatest kolmanda isiku isikuandmetest ja võimalikust riivest kolmanda isiku õigustele lihtsalt teadlikuks – üldmäärus ei kohusta teda andmeid läbi vaatama ega ülekantavate andmetega sisuliselt tutvuma.

Eeltoodu põhjal leiab kinnitust ka magistritöös püstitatud teine hüpotees, et vastutaval töötlejal ei ole võimalik keelduda kolmanda isiku õiguste ja vabaduste kaitse põhjendusel andmesubjekti esitatud andmete ülekandmise taotluse täitmisest.

3.3.Uue vastutava töötleja õiguslik alus kolmanda isiku isikuandmete töötlemiseks

Juhul, kui andmesubjekti esitatud andmete ülekandmise taotluse alusel kantakse teise vastutava töötleja juurde üle andmed, milles sisalduvad ka kolmandat isikut puudutavad isikuandmed, siis tekib küsimus, kas uuel vastutaval töötlejal on õiguslik alus kolmanda isiku isikuandmete töötlemiseks.

Andmesubjekt, kes on üldmääruse artikli 20 alusel andmete ülekandmist taotlenud, saab omal vabal tahtel valida uue vastutava töötleja (olgu see siis nt mõni sotsiaalmeedia teenusepakkuja), kelle juurde andmed üle kanda soovib. Kuna andmesubjekt valib teadlikult uue vastutava töötleja, siis peab ta uuele vastutavale töötlejale andma nõusoleku isikuandmete töötlemiseks või sõlmima lepingu, mis annab uuele vastutavale töötlejale õigusliku aluse andmesubjekti isikuandmete töötlemiseks.[151] Kolmanda isiku isikuandmete ülekandmisel aga uuel vastutaval töötlejal õiguslik alus teise isiku isikuandmete töötlemiseks puudub, sest kolmas isik ei kanna oma isikuandmeid vabal tahtel uue vastutava töötleja juurde üle, vaid need jõuavad uue

[151] Samal seisukohal on ka artikli 29 töörühm, öeldes: „Andmesubjekt, kes algatab oma andmete edastamise teisele vastutavale töötlejale, annab uuele vastutavale töötlejale töötlemiseks nõusoleku või sõlmib temaga lepingu.“ – Artikli 29 töörühm, lk 11.

vastutava töötlejani andmesubjekti esitatud andmete ülekandmise taotluse tõttu. Seetõttu on vaatluse all just õiguslik alus kolmanda isiku isikuandmete töötlemiseks.

Artikli 29 töörühm on andmete ülekandmise õiguse kohta antud suunises selgitanud: „Andmesubjekt, kes algatab oma andmete edastamise teisele vastutavale töötlejale, annab uuele vastutavale töötlejale töötlemiseks nõusoleku või sõlmib temaga lepingu. Kui andmekogum sisaldab kolmandate isikute isikuandmeid, tuleb töötlemiseks kindlaks määrata mõni muu õiguslik alus. Näiteks võib vastutav töötleja artikli 6 lõike 1 punkti f alusel tugineda õigustatud huvile, eelkõige kui vastutava töötleja eesmärk on pakkuda andmesubjektile teenust, mis võimaldab viimasel töödelda isikuandmeid eranditult isiklikel või kodustel eesmärkidel. Töötlemistoimingute eest, mille andmesubjekt algatab isikliku tegevuse käigus ning mis puudutavad ja võivad mõjutada kolmandaid isikuid, vastutab andmesubjekt sel määral, mil vastutav töötleja ei tee töötlemise kohta mingil viisil otsuseid.“[152]

Üldmääruse artikkel 6 lg 1 p f sätestab: *Isikuandmete töötlemine on seaduslik ainult juhul, kui on täidetud vähemalt üks järgmistest tingimustest, ning sellisel määral, nagu see tingimus on täidetud: isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja –vabadused, mille nimel tuleb kaitsta isikuandmeid, eriti juhul kui andmesubjekt on laps.*

Õigustatud huvi selgitab täpsemalt üldmääruse põhjenduspunkt 47: „Töötlemise õiguslikuks aluseks võib olla vastutava töötleja (sealhulgas sellise vastutava töötleja, kellele võidakse isikuandmeid avaldada, või kolmanda isiku) õigustatud huvi, tingimusel et andmesubjekti huvid või põhiõigused ja -vabadused ei ole tähtsamad, võttes arvesse andmesubjekti mõistlikke ootusi, mis põhinevad tema suhtel vastutava töötlejaga. Selline õigustatud huvi võib olemas olla näiteks siis, kui andmesubjekti ja vastutava töötleja vahel on asjakohane ja sobiv suhe, näiteks kui andmesubjekt on vastutava töötleja klient või töötab tema teenistuses. Igal juhul tuleks õigustatud huvi olemasolu hoolikalt hinnata, sealhulgas seda, kas andmesubjekt võib andmete kogumise ajal ja kontekstis mõistlikkuse piires eeldada, et isikuandmeid võidakse sellel otstarbel töödelda. Andmesubjekti huvid ja põhiõigused võivad olla vastutava töötleja huvidest tähtsamad eelkõige juhul, kui isikuandmeid töödeldakse olukorras, kus andmesubjektil ei ole mõistlik eeldada edasist töötlemist. /.../“[153]

[152] Artikli 29 töörühm, lk 11.
[153] Üldmäärus, põhjenduspunkt 47.

Artikli 29 töörühma pakutud lahendust saab pidada põhjendatuks: juhul kui ülekantavad andmed sisaldavad kolmandate isikute isikuandmeid ja need kantakse üle teise vastutava töötleja juurde, tuleks uuel vastutaval töötlejal leida õiguslik alus kolmanda isiku isikuandmete töötlemiseks, nt tugineda õigustatud huvile. Õigustatud huvi võib kõne alla tulla siis, kui a) muu õiguslik alus ei ole töötlemise iseloomu ja/või ulatuse tõttu saadaval; või b) võimalik on tugineda ka muudele õiguslikele alustele, kuid õigustatud huvi on kõige asjakohasem.[154]

Kõikidest üldmääruse artiklis 6 sätestatud õiguslikest alustest on üldmääruse artikli 6 lg 1 p-s f sätestatud õigustatud huvi autori hinnangul andmete ülekandmise õiguse iseloomust tulenevalt ainus, millele uus vastutav töötleja saaks kolmanda isiku isikuandmete töötlemisel tugineda. Muu õiguslik alus ei ole töötlemise iseloomu tõttu saadaval, sest vastutav töötleja on andmed saanud mujalt kui kolmandalt isikult. Uue vastutava töötleja silmis on kolmas isik samuti andmesubjektiks samuti nagu esialgne andmesubjekt, kes andmete ülekandmise õigust taotles ning uus vastutav töötleja vajab õiguslikku alust, et tema isikuandmeid seaduslikult töödelda. Uus vastutav töötleja ei ole kolmanda isikuga otseses õigussuhtes, sest puudub andmesubjekti nõusolek (üldmääruse artikkel 6 lg 1 p a) või andmesubjekti osalusel sõlmitud leping (artikkel 6 lg 1 p b). Samuti pole töötlemine vajalik vastutava töötleja juriidilise kohustuse täitmiseks (artikkel 6 lg 1 p c) ega andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks (artikkel 6 lg 1 p d). Ühtlasi ei ole töötlemine vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks (artikkel 6 lg 1 p e). Muudest nimetatud alustest ei tulene seega vastutavale töötlejale õiguslikku alust kolmanda isiku isikuandmete töötlemiseks.

Üldmääruse artikli 6 lg 1 p f alusel õigustatud huvile tuginemiseks peab vastutav töötleja läbi viima nö õigustatud huvi hindamise testi,[155] kusjuures vastutav töötleja peab arvestama, et ta peab suutma tõendada õigustatud huvi olemasolu.[156] Seega tuleks vastutaval töötlejal õigustatud huvi hindamise test kohaselt dokumenteerida. Kolmeastmelise testi abil tuleb vastutaval töötlejal hinnata õigustatud huvi olemasolu, töötlemise vajalikkust ja andmesubjekti ja vastutava töötleja õiguste ja huvide tasakaalustatust. Autor hindab neid aspekte alljärgnevas:

1. Eesmärgipärasuse test (ingl k *purpose test*) ehk õigustatud huvi kindlakstegemine

[154] Data Protection Network. Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation, 06.04.2018, lk 7.
[155] S. Velbri. Isikuandmete kaitse üldmäärusest tulenev nõusoleku vajadus ja selle tingimused isikuandmete töötlemisel äriühingute poolt. Magistritöö. Tallinn: Tartu ülikooli õigusteaduskond 2018, lk 29.
[156] P. Voigt, A. von dem Bussche, lk 103.

Uus vastutav töötleja peab esmalt kindlaks tegema kolmandat isikut puudutavate isikuandmete töötlemise eesmärgi[157] ja tuvastama, kas tal esineb õigustatud huvi isikuandmete töötlemiseks. Õigustatud huvi võib olla mis tahes huvi, mis on seadusega kooskõlas ning mida võib seetõttu laialt tõlgendada.[158]

Kui uue vastutava töötleja juurde kantakse üle ka kolmanda isiku isikuandmeid sisaldavad andmed, peaks uue vastutava töötleja eesmärk kolmandat isikut puudutavate isikuandmete töötlemisel olema tagada andmete säilimine kujul, millel nad uuele vastutavale töötlejale esitati. Sama põhimõtet kinnitab ka AKI seisukoht andmete ülekandmise osas. AKI antud isikuandmete töötleja üldjuhendis rõhutatakse, et mis tahes juhul tohib uus vastutav töötleja töödelda andmete ülekandmise õiguse täitmisel saadud andmeid üksnes algsel eesmärgil. Täpsemalt on AKI juhendis selgitatud: „Näiteks kui inimene on e-posti teenuses salvestanud sõprade, tuttavate või sugulaste kontaktandmed ning palub olemasoleval teenusepakkujal need edastada uuele teenusepakkujale, võib viimane neid andmeid töödelda ainult algsel eesmärgil, milleks on kontaktandmete säilimise tagamine. Sama kehtib ka inimese maksetehingute ajalooga, mis kantakse olemasolevast pangast uude. Nii uus pank kui e-posti teenusepakkuja ei tohi pangatehingus osalenud teiste inimeste andmeid või e-posti kontaktide nimekirja automaatselt kasutada näiteks oma teenuste pakkumiste või muude otseturustussõnumite edastamiseks.“[159]

Isikuandmete töötlemise eesmärgi piirangu põhimõtte sätestab üldmääruse artikkel 5 lg 1 p b: *isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus /.../ („eesmärgi piirang“).*

Uue vastutava töötleja õigustatud huvi seisneb andmete kogumisest ja töötlemisest saadavas kasus. Sellele annab kinnitust ka üks andmete ülekandmise õiguse majanduslikest eesmärkidest saavutada ühisturul suurem konkurents vastutavate töötlejate vahel (vt lähemalt käesoleva töö alapeatükk 1.3). Andmete liikumine vastutavate töötlejate vahel võimaldab saavutada ühisturul suuremat konkurentsi, mis viitab sellele, et ülekantavad andmed kannavad endas vastutava töötleja jaoks teatavat väärtust või kasu, mille saamise vastu võib vastutaval töötlejal olla õigustatud huvi. Seega saab olla vastutava töötleja õigustatud huviks saada andmete kogumisest ja töötlemisest kasu ning töötlemise eesmärk on andmete säilimise tagamine.

[157] Data Protection Network. Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation, 06.04.2018, lk 17.
[158] P. Voigt, A. von dem Bussche, lk 103.
[159] Andmekaitse inspektsioon, lk 37.

Autori hinnangul on tuvastatav uue vastutava töötleja õigustatud huvi olemasolu kolmanda isiku isikuandmete töötlemiseks.

2. Vajalikkuse test (ingl k *necessity test*)

Vastutav töötleja peab teiseks hindama, kas on olemas mõni muu alternatiivne võimalus saavutamaks tuvastatud huvi või eesmärki ilma kõnesolevat töötlemist teostamata.[160]

Käesolev punkt seondub kõige enam uue vastutava töötleja poolt kolmanda isiku isikuandmete töötlemise seaduslikkuse tagamisega, misläbi saab uus vastutav töötleja tagada andmete säilimise sel kujul, millel need talle esitati ja tagada töötlemise vastavus õigusaktidest (eelkõige üldmäärusest) tulenevatele nõuetele.

Autori hinnangul ei ole vastutaval töötlejal võimalust tagada kolmanda isiku isikuandmete töötlemist mõnel muul õiguslikul alusel. Kõikide muude üldmääruse artikli 6 lg 1 p-dest a kuni f tulenevatele õiguslikele alustele tuginemine on välistatud, sest uus vastutav töötleja on andmed saanud teiselt vastutavalt töötlejalt andmete ülekandmise õiguse täitmise tõttu, mis ei sobitu ühegi muu õigusliku alusega. Kuna muid võimalusi uue vastutava töötleja jaoks kolmanda isiku isikuandmete töötlemiseks ei esine, on töötlemine õigustatud huvi alusel vajalik.

3. Tasakaalustatuse test (ingl k *balancing test*)

Kolmandaks peab vastutav töötleja tasakaalustatuse testi läbi viies hindama, kas kolmanda isiku huvid või põhiõigused ja -vabadused oleksid tähtsamad kui vastutava töötleja õigustatud huvi kolmanda isiku isikuandmete töötlemiseks.[161] Et teha kindlaks, kas kolmanda isiku õigused ja vabadused (eelkõige tema õigus privaatsusele[162]) on tähtsamad kui uue vastutava töötleja õigustatud huvi, tuleb hinnata, millised on kolmanda isiku isikuandmete töötlemise tagajärjed kolmanda isiku jaoks ning millises ulatuses kahjustusi teise isiku õigustele ja vabadustele võib kolmanda isiku isikuandmete töötlemine kaasa tuua.[163]

Üldmääruse artikli 5 lg 1 p-s b sätestatud eesmärgi piirangu põhimõttest tulenevalt peab uus vastutav töötleja tagama isikuandmete kogumise täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ja vältima nende hilisemat töötlemist viisil, mis on nende eesmärkidega vastuolus. Sellest tuleneb uuele vastutavale töötlejale kaks kohustust. Esiteks on uuel vastutaval töötlejal kohustus talle üle kantud isikuandmete töötlemine samal eesmärgil,

[160] Data Protection Network, lk 17.
[161] Data Protection Network, lk 17.
[162] P. Voigt, A. von dem Bussche, lk 105.
[163] P. Voigt, A. von dem Bussche, lk 106.

milleks neid varem töödeldi. Näiteks ei tohiks uus vastutav töötleja kasutada kolmandat isikut puudutavaid isikuandmeid otseturunduse eesmärgil.[164] Samuti ei tohi uus vastutav töötleja kasutada kolmandate isikute kohta edastatud andmeid oma tarbeks, nt neile turundustoodete ja –teenuste soovitamiseks ega kolmanda isiku teadmise ja nõusolekuta tema profiili täiendamiseks ja tema sotsiaalse keskkonna ümberkujundamiseks.[165] Teiseks tuleb uuel vastutaval töötlejal tagada, et töötleb talle üle kantud isikuandmeid täpselt samal viisil, kuidas neid töötles endine vastutav töötleja.

Üldmääruse artikkel 5 lg 1 p sätestab isikuandmete töötlemise põhimõttena ka võimalikult väheste andmete kogumise põhimõtte (nn minimaalsuse põhimõtte), et isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt. See ei tähenda, et vastutaval töötlejal on kohustus viia andmete töötlemine täieliku miinimumini, vaid piirata andmete kogumist vaid üksnes eesmärgi täitmiseks vajaliku tasemeni.[166] Selle järgi peaks uus vastutav töötleja jätkama andmete töötlemist samal eesmärgil nagu eelmine vastutav töötleja, näiteks üksnes andmete säilitamiseks, ning andmete töötlemise eesmärki mitte omal valikul muutma. Vastasel korral on selline töötlemine tõenäoliselt ebaseaduslik ja ebaõiglane, eriti kui asjaomaseid isikuid ei teavitata ja nad ei saa andmesubjektidena oma õigusi teostada.[167]

Kui uus vastutav töötleja lähtub üldmääruses sätestatud isikuandmete töötlemise põhimõtetest, pidades eriti silmas eesmärgi piirangu põhimõtet ja minimaalsuse põhimõtet, ei ole tõenäoline, et töötlemine põhjustaks kolmandale isikule põhjendamatut kahju. Seega võib öelda, et juhul kui uus vastutav töötleja jätkab andmete töötlemist samal eesmärgil nagu eelmine vastutav töötleja, siis ei kahjustaks uue vastutava töötleja poolt õigustatud huvi alusel kolmanda isiku isikuandmete töötlemine kolmanda isiku õigusi ja vabadusi, eelkõige kolmanda isiku õigust eraelu puutumatusele ja isikuandmete kaitsele.

Tasakaalustatuse testi raames võib analüüsida mitmeid aspekte, sh ka seda, kas kolmas isik oskab oodata või eeldada tema isikuandmete töötlemist uue vastutava töötleja poolt. Suure tõenäosusega ei tea kolmas isik, et tema isikuandmed andmesubjekti esitatud taotluse alusel teise vastutava töötleja juurde üle kanti. Lisaks ei ole kolmanda isiku ja uue vastutava töötleja vahel varasemat omavahelist suhet.

[164] Artikli 29 töörühm, lk 11-12.
[165] Artikli 29 töörühm, lk 12.
[166] P. Voigt, A. von dem Bussche, lk 90.
[167] Artikli 29 töörühm, lk 12.

Samas on üldmääruse üheks läbivaks põhimõtteks andmesubjekti õiguste puhul see, et isik saab oma andmete üle kontrolli teostada, kasutades üldmäärusest tulenevaid andmesubjekti õigusi üksnes juhul, kui ta on üleüldse teadlik asjaolust, et tema isikuandmeid töödeldakse.[168] Juhul kui andmete ülekandmise õigust teostades kantakse üle ka kolmandat isikut puudutavad isikuandmed (ning selline olukord ei ole üldmääruse artikliga 20 sätestatud andmete ülekandmise õiguse regulatsiooniga täielikult välistatud), ei saa kolmas isik teadlikuks, et tema isikuandmed on üle kantud teise vastutava töötleja juurde. Seetõttu ei ole tal ka võimalik teostada üldmäärusest tulenevaid andmesubjekti õigusi.

Uue vastutava töötleja poolt õigustatud huvile tuginemine võib aga olla kolmandale isikule kasulik, sest õigustatud huvile tuginemine toob kaasa üldmääruse artiklis 14 sisalduva uue vastutava töötleja poolt andmesubjekti teavitamise kohustuse, mis omakorda annab kolmandale isikule taas kontrolli tema isikuandmete töötlemise üle. Nimelt tuleneb üldmääruse artiklist 14 vastutava töötleja kohustus teavitada andmesubjekti tema isikuandmete töötlemisest vastutava töötleja poolt, kui andmed ei ole saadud andmesubjektilt. Andmete ülekandmise õiguse puhul ei ole uus vastutav töötleja saanud andmeid andmesubjektilt endalt, vaid andmete ülekandmise teostamisel eelmiselt vastutavalt töötlejalt. Lühidalt öeldes tuleb vastutaval töötlejal üldmääruse artikli 14 alusel teavitada andmesubjekti tema isikuandmete töötlemisest, informeerida teda vastutava töötleja andmetest, teavitada teda mh töötlemise eesmärgist ja õiguslikust alusest ja asjaomaste isikuandmete liigist.[169] Sama sätte lg 3 p a sätestab, et vastutav töötleja esitab lõigetes 1 ja 2 osutatud teabe mõistliku aja jooksul pärast isikuandmete saamist, kuid hiljemalt ühe kuu jooksul, võttes arvesse isikuandmete töötlemise konkreetseid asjaolusid. Üldmääruse artikliga 14 kehtestatud teavitamise kohustust tuleb täita andmete ülekandmise õiguse teostamisel uuel vastutaval töötlejal, misläbi tagatakse, et kolmas isik oleks teadlik tema isikuandmete töötlemisest uue vastutava töötleja poolt. Sel viisil on teisel isikul võimalik ka teostada üldmäärusest tulenevaid andmesubjekti õigusi.

Teave tuleb isikule esitada hiljemalt ühe kuu jooksul võttes arvesse konkreetse töötlemise asjaolusid, välja arvatud: a) isikul on see teave juba olemas; b) teabe esitamine on võimatu või nõuab ebaproportsionaalseid pingutusi (nt teadusuuringute ja statistika puhul); c) isikuandmete saamine või avaldamine on sätestatud seadusega või; d) isikuandmed on kaetud saladuse hoidmise kohustusega.[170] Niisiis tuleb õigustatud huvile tuginemisel uue vastutava töötleja

[168] P. Voigt, A. von dem Bussche. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing AG 2017, lk 147.
[169] Üldmäärus, artikkel 14 lg 1.
[170] Andmekaitse inspektsioon, lk-d 48-49.

poolt igal üksikjuhul vastavalt asjaoludele hinnata, ega ei esine teavitamiskohustust välistavaid asjaolusid.

Artikli 29 töörühm on selgitanud: „Teiste (nõusolekut mitte andnud) andmesubjektide /.../ kahjustamine toimuks näiteks juhul, kui andmete edastamine ühelt vastutavalt töötlejalt teisele takistaks kolmandatel isikutel teostada andmesubjektidena oma isikuandmete kaitse üldmääruse kohaseid õigusi (nagu õigus saada teavet, õigus tutvuda andmetega jne).[171] Üldmääruse artiklist 14 tuleneva teavitamise kohustuse täitmisel ei kahjustaks vastutav töötleja kolmanda isiku õigusi, sest teavitamise abil saaks ta teadlikuks oma isikuandmete töötlemisest ning tal oleks uue vastutava töötleja juures võimalik kasutada üldmäärusest tulenevaid andmesubjekti õigusi.

Kolmanda isiku teavitamise vajadust toetab ka üldmääruse põhjenduspunktis 58 kirjeldatud läbipaistvuse põhimõte, mille järgi üldsusele või andmesubjektile suunatud teave on kokkuvõtlik, lihtsalt kättesaadav ja arusaadav ning selgelt ja lihtsalt sõnastatud. Eriti asjakohane on see muudes olukordades, mille puhul osapoolte arvukuse ja kasutatava tehnoloogia keerukuse tõttu on andmesubjektil raske teada saada ja mõista, kas tema isikuandmeid kogutakse, kes neid kogub ja millisel eesmärgil.[172] Et kolmandal isikul oleks võimalik mõista, kas tema isikuandmeid kogutakse, on teavitamise kohustusel eriti oluline roll.

Järelikult võib uue vastutava töötleja poolt õigustatud huvile tuginemine olla lõppastmes hoopis kolmandale isikule kasulik, sest seeläbi saab ta teadlikuks tema isikuandmete töötlemisest. Samuti tekib tal sel juhul võimalus kontrollida oma isikuandmete töötlemist ja teostada üldmäärusest tulenevaid andmesubjekti õigusi. Seetõttu ei kahjusta uus vastutav töötleja õigustatud huvile tuginedes kolmanda isiku õigusi.

Kokkuvõttes ei kaalu kolmanda isiku õigused, eelkõige tema õigus eraelu puutumatusele ja isikuandmete kaitsele, üles uue vastutava töötleja õigustatud huvi tema isikuandmete töötlemiseks, sest lõppastmes annab õigustatud huvile tuginemine kolmandale isikule kontrolli tema isikuandmete töötlemise üle ja tal on võimalik isikuandmete töötlemise suhtes teostada üldmäärusest tulenevaid andmesubjekti õigusi. Seetõttu on uuel vastutaval töötlejal võimalik kolmanda isiku isikuandmete töötlemisel tugineda üldmääruse artikli 6 lg 1 p-le f ehk töödelda tema isikuandmeid õigustatud huvi alusel.

Eeltoodu põhjal selgub, et kinnitust leiab ka magistritöös püstitatud kolmas hüpotees, et kui andmete ülekandmise õiguse teostamisel kantakse uue vastutava töötleja juurde üle ka

[171] Artikli 29 töörühm, lk 11.
[172] Üldmäärus, põhjenduspunkt 58.

kolmanda isiku isikuandmed, kaotab kolmas isik oma isikuandmete üle kontrolli ega saa kasutada üldmäärusest tulenevaid andmesubjekti õigusi, välja arvatud juhul, kui uus vastutav töötleja määrab kolmanda isiku isikuandmete töötlemisele õigusliku aluse ja teavitab sellest uut andmesubjekti.

Kolmas kinnitust leidnud hüpotees omab käesoleva magistritöö seisukohalt väga positiivset tulemust kolmandate isikute õiguste kaitse seisukohalt. Leitu sisuline väärtus on see, et juhul kui andmete ülekandmise õiguse teostamisel kantakse uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed, tuleks uuel vastutaval töötlejal leida õiguslik alus kolmanda isiku isikuandmete töötlemiseks. Kõige sobivamaks õiguslikuks aluseks selles olukorras on tugineda üldmääruse artikli 6 lg 1 p-s f sätestatud õigustatud huvile. Õigusliku aluse määratlemine kolmanda isiku isikuandmete töötlemiseks toob kaasa ka uue vastutava töötleja üldmääruse artiklist 14 tuleneva kohustuse teavitada andmesubjekti tema isikuandmete töötlemisest. Selle abil saab kolmas isik teada tema isikuandmete töötlemisest uue vastutava töötleja juures ja tal on taas võimalik teostada kontrolli oma isikuandmete üle. Ühtlasi saab seda pidada ainsaks autori poolt tuvastatud üldmäärusest tulenevaks õiguslikuks meetmeks ja võimaluseks, mis tagab kolmanda isiku teadlikkuse tema isikuandmete töötlemisest ja võimaluse teostada oma isikuandmete üle kontrolli andmete ülekandmise korral.

KOKKUVÕTE

Andmete ülekandmise õigus on üldmääruses sisalduv uudne andmesubjekti õigus saada vastutavalt töötlejalt koopia teda puudutavatest isikuandmetest, edastada need andmed teisele vastutavale töötlejale või nõuda vastutavalt töötlejalt andmete otse ülekandmist teise vastutava töötleja juurde, kui see on tehniliselt teostatav. Andmete ülekandmise õiguse teostamisel võib aga esineda olukordi, kus andmesubjekti taotlusel kantakse ühes andmesubjekti puudutavate isikuandmetega teise vastutava töötleja juurde üle ka kolmanda isiku isikuandmed. Seetõttu esineb oht, et kolmas isik kaotab oma isikuandmete üle kontrolli, sest ta ei saa teadlikuks, et tema isikuandmed on üle kantud teise vastutava töötleja juurde. Kolmandal isikul ei ole seetõttu võimalik teostada teda puudutavate andmete suhtes üldmäärusest tulenevaid andmesubjekti õigusi.

Magistritöö eesmärgiks oli analüüsida andmete ülekandmise õiguse sisu, eesmärki, eelduseid, seost muude andmesubjekti õigustega ja vastutavate töötlejate kohustusi andmete ülekandmisel. Samuti oli töö fookuses kolmandate isikute õigus eraelu puutumatusele ja isikuandmete kaitsele juhul, kui andmete ülekandmise õiguse teostamisel kantakse ühes andmesubjekti andmetega uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmeid. Sellega seonduvalt otsisin kinnitust kolmele magistritöös püstitatud hüpoteesile. Esiteks, andmete ülekandmise õiguse teostamine riivab kolmandate isikute eraelu puutumatuse ja isikuandmete kaitse õigust, kui andmete ülekandmise õiguse teostamisel kantakse uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed. Teiseks, vastutaval töötlejal ei ole võimalik keelduda kolmanda isiku õiguste ja vabaduste kaitse põhjendusel andmesubjekti esitatud andmete ülekandmise taotluse täitmisest. Kolmandaks, kui andmete ülekandmise õiguse teostamisel kantakse uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed, kaotab kolmas isik oma isikuandmete üle kontrolli ega saa kasutada üldmäärusest tulenevaid andmesubjekti õigusi, välja arvatud juhul, kui uus vastutav töötleja määrab kolmanda isiku isikuandmete töötlemisele õigusliku aluse ja teavitab sellest uut andmesubjekti.

Esimeses peatükis analüüsisin andmete ülekandmise õiguse sisu, selgitades, et andmete ülekandmise õigus koosneb kolmest elemendist: esiteks on andmesubjektil õigus saada vastutava töötleja käest koopia andmesubjekti puudutavatest isikuandmetest, mida vastutav töötleja tema kohta hoiab (artikkel 20 lg 1), teiseks on andmesubjektil õigus saadud andmed ise teise vastutava töötleja juurde üle kanda (artikkel 20 lg 1), ning kolmandaks on andmesubjektil õigus nõuda andmete otse ülekandmist ühe vastutava töötleja juurest teise juurde, kui see on tehniliselt teostatav (artikkel 20 lg 2). Samuti tuvastasin, et andmete ülekandmise taotluse esitamine ei piira andmesubjekti õigust esitada samale vastutavale töötlejale muid üldmääruses

kehtestatud andmesubjekti õigustest tulenevaid taotlusi. Andmete ülekandmise õiguse eesmärgid on tugevdada andmesubjekti kontrolli teda puudutavate isikuandmete üle (nn andmekaitseline eesmärk), vältida andmesubjekti nn „kinnijäämist“ ühe teenusepakkuja juurde ja saavutada EL ühisturul suurem konkurents vastutavate töötlejate vahel (nn majanduslikud eesmärgid).

Esimeses peatükis andsin ka vastuse küsimusele, millised on eeldused andmete ülekandmise õiguse teostamiseks. Kõik eeldused peavad esinema samaaegselt. Esiteks, isikuandmete töötlemine peab põhinema andmesubjekti nõusolekul või lepingul, mis tähendab, et juhul kui andmesubjekti isikuandmeid töödeldakse mõnel muul õiguslikul alusel, ei saa andmesubjekt nõuda vastutavalt töötlejalt andmete ülekandmist. Teiseks, isikuandmete töötlemine on automatiseeritud, ehk andmete ülekandmise õiguse kohaldamisalasse kuuluvad üksnes isikuandmed, mida töödeldakse tehnoloogia abil, mitte paberkandjal. Kolmandaks, isikuandmed puudutavad konkreetset andmesubjekti, mille all tuleb mõista üldmääruse artiklil 4 p 1 tuginedes teavet tuvastatud või tuvastatava füüsilise isiku kohta. Neljandaks, isikuandmed on andmesubjekti enda poolt vastutavale töötlejale esitatud, mille puhul tuleb eelistada laiemat tõlgendust. Üksnes järeldatud või tuletatud andmed tuleb andmete ülekandmise õiguse kohaldamisalast välja arvata. Andmed, mille vastutav töötleja on andmesubjekti kohta ise kogunud, ei kuulu andmesubjekti poolt esitatud andmete hulka ega ole andmete ülekandmise õiguse objektiks. Viiendaks, ei tohi andmete ülekandmise õiguse teostamine kahjustada teiste isikute õigusi ja vabadusi (artikkel 20 lg 4). Autori hinnangul esineb üldmääruse artikli 20 lg-s 4 tõlkeviga ning selle korrektne tõlge eesti keelde oleks: lõikes 1 osutatud õigus ei tohi kahjustada teiste isikute õigusi ja vabadusi.

Vastutava töötleja peamised kohustused andmete ülekandmisel on üldmääruse artikli 20 lg 1 järgi mitte takistada andmete ülekandmist, artikli 12 lg-st 5 tulenevalt esitada andmesubjektile andmed tasuta ja artikli 12 lg-st 3 tulenevalt tarbetu viivituseta hiljemalt ühe kuu jooksul pärast taotluse saamist. Vastutavatel töötlejatel ei ole kohustust hoida töös tehniliselt ühilduvaid andmesüsteeme, kuid neid suunatakse kasutama koostalitlevaid vorminguid. Artikli 29 töörühm on viidanud ka vastutava töötleja kohustusele kontrollida, et andmeid vastuvõttev vastutav töötleja tegutseb andmesubjekti nimel, kuid üldmääruse tekst sellist kohustust ei sätesta. Viimaks on vastutaval töötlejal üldmääruse artiklist 12 tulenev kohustus teavitada andmesubjekti tema isikuandmete töötlemisest.

Eraldi analüüsisin andmeid vastuvõtva vastutava töötleja ehk uue vastutava töötleja kohustusi. Leidsin, et uuele vastutavale töötlejale kohalduvad kõik kohustused, mis kohalduvad ka andmed saatnud vastutavale töötlejale. Uutel vastutavatel töötlejatel on kohustus järgida kõiki

üldmääruse artiklis 5 sätestatud isikuandmete töötlemise põhimõtteid: võimalikult väheste andmete kogumise põhimõtte kohaselt peab uus vastutav töötleja kindlaks tegema, et talle üle kantud andmed on asjakohased. Seda saab ta aga teha üksnes juhul, kui ta saadud andmetega ka sisuliselt tutvub. Eesmärgi piirangust lähtudes võib väita, et uus vastutav töötleja peab talle üle kantud andmetega sisuliselt tutvuma selleks, et määratleda saadud andmete töötlemise eesmärk. Seetõttu leidsin, et uuel vastutaval töötlejal tuleb saadud andmetega sisuliselt tutvuda. Juhul, kui uus vastutav töötleja määratleb õigusliku aluse kolmanda isiku isikuandmete töötlemiseks, on uus vastutav töötleja artiklist 14 tulenevalt kohustatud teda teavitama isikuandmete töötlemisest.

Ühtlasi võib andmete ülekandmise õiguse teostamisel esineda turvarisk, et juhul kui vastutav töötleja ei suuda korrektselt identifitseerida andmesubjekti isikut, väljastab ta andmed isikule, keda andmed tegelikult ei puuduta. See võib anda võimaluse kuritarvitusteks. Autori soovitusena tuleks vastutavatel töötlejatel kehtestada kohased autentimismenetlused taotluse esitanud isiku tuvastamiseks. Lisaks tuleks üldmääruse artikleid 11, 12 ja 32 koos tõlgendades tunnustada vastutava töötleja kohustust tuvastada taotluse esitanud isik, mida üldmäärus eraldi ja otsesõnu ei sätesta.

Teise peatüki fookus oli teha kindlaks, kas andmete ülekandmise õigus riivab kolmanda isiku õigust eraelu kaitsele ja isikuandmete kaitsele. Mõlema õiguse riivet on analüüsitud üheskoos, lähtudes EK praktikas kujundatud metoodikast, mille põhjal lahendatakse kaasuseid, kus on üheaegselt võimalik riive nii eraelu puutumatuse kui ka isikuandmete kaitse õigustele. Esiteks selgus, et andmete ülekandmise õiguse teostamine langeb kolmanda isiku õiguse isikuandmete kaitsele ja eraelu kaitsele esemelisse kohaldamisalasse, juhul kui tegemist on kolmanda isiku isikuandmetega, nende andmete kogumine ja kasutamine asjassepuutuva asutuse poolt ja nende edastamine kolmandale isikule on isikuandmete töötlemine ning esineb isiku eraellu sekkumine. Leidsin, et kolmanda isiku eraellu sekkumine esineb juhul, kui teda puudutavad isikuandmed edastatakse uuele vastutavale töötlejale ning selliste isikuandmete edastamisel, avalikustamisel või mis tahes muul toimingul on seos kolmanda isiku eraeluga. Teiseks selgus, et andmesubjekti puudutavate isikuandmetega ühes kolmandate isikute isikuandmete ülekandmine uue vastutava töötleja juurde kujutab endast riivet kolmanda isiku õigusele eraelu puutumatusele ja isikuandmete kaitsele.

Seega leidis teises peatükis kinnitust magistritöö esimene hüpotees, et andmete ülekandmise õigus riivab teise isiku õigust eraelu kaitsele ja isikuandmete kaitsele, kui andmete ülekandmise õiguse teostamisel kantakse üle ka teise isiku isikuandmed. Hüpoteesi kinnitamiseni viis arutluskäik, et andmete ülekandmise õiguse teostamisel kolmanda isiku isikuandmeid üle

kandes sekkutakse alati isiku eraellu. Eriti tõsiseks saab sekkumist pidada juhul, kui kolmanda isiku isikuandmed edastatakse või avalikustatakse piiratud või piiramata isikute ringile. Üks andmete ülekandmise õiguse eesmärke – anda andmesubjektile suurem kontroll tema isikuandmete üle – on iseenesest legitiimne eesmärk, kuid andmete ülekandmise õigust teostades (juhul, kui selle raames kantakse üle kolmanda isiku isikuandmed) sekkutakse alati vähemal või suuremal määral kolmanda isiku õigusesse eraelu kaitsele ja isikuandmete kaitsele. Teine andmete ülekandmise õiguse eesmärk – edendada EL majandust (ka nn üldist huvi pakkuv eesmärk) – ei ole autori hinnangul legitiimne eesmärk, sest majanduslikke eesmärke ei saa asetada isikute õiguste ja vabaduste kaitsest kõrgemale. Kolmandat andmete ülekandmise õiguse eesmärki – vältida andmesubjekti nn kinnijäämist ühe vastutava töötleja juurde, ei saa samuti pidada legitiimseks eesmärgiks, sest juhul kui andmete ülekandmisel sisalduvad andmekogumis kolmandate isikute isikuandmed, ei arvesta see kolmandate isikute õiguste ja vabadustega. Õiglane lahendus kolmandate isikute õiguste ja vabadustega arvestamiseks oleks see, kui üldmäärus sätestaks, kuidas saavad kolmandad isikud ülekantud andmete osas kontrolli teostada, kuid selline regulatsioon üldmääruses puudub.

Kolmandas peatükis keskendusin küsimusele, kuidas kaitstakse kolmandate isikute õigusi ja vabadusi, kui riivatakse nende õigust eraelu puutumatusele ja isikuandmete kaitsele. Samuti, millised abinõud on kolmandate isikute õiguste ja vabaduste kaitseks üldmääruses ette nähtud. Esimeseks uurimistulemuseks oli, et artikli 29 töörühma suunis andmete eraldatavuseks tehnilise lahenduse loomiseks ei oma tähtsust kolmandate isikute õiguste ja vabaduste kaitsel, sest see ei võimalda andmekogumist kolmandate isikute isikuandmete eraldamist, vaid üksnes kaudsete ja süsteemi loodud andmete eraldamist.

Järgnevalt analüüsisin kolmandas peatükis vastutava töötleja õigust keelduda andmesubjekti esitatud andmete ülekandmise taotlusest, mida saab üldmääruse artikkel 12 lg 5 alusel teha üksnes juhul, kui andmesubjekti taotlus on selgelt põhjendamatu või ülemäärane, eelkõige oma korduva iseloomu tõttu. Andmete ülekandmise õiguse eripära võrreldes teiste andmesubjekti õigustega on võimaldada andmete ülekandmist sobiva tehnilise lahenduse abil. Seetõttu ei peaks vastutav töötleja korduva iseloomuga taotlustest ülemäärasuse põhjendusel keelduma, sest korduvate taotluste täitmist aitab lihtsustada sobiva tehnilise lahenduse olemasolu. Et tugineda teisele keeldumise alusele, et andmesubjekti esitatud taotlus on selgelt põhjendamatu, peab vastutavale töötlejale ilmnema, et tal on objektiivselt võimatu andmesubjekti taotlust täita. Lisaks leidis tuvastamist, et vastutav töötleja ei saa andmetes sisalduvatest kolmandate isikute isikuandmetest lihtsalt teadlikuks, sest üldmäärus ei kohusta teda andmetega sisuliselt tutvuma. Neil põhjendustel leidis kinnitust magistritöös püstitatud teine hüpotees, et vastutaval töötlejal

ei ole võimalik keelduda teise isiku õiguste ja vabaduste kaitse põhjendusel andmesubjekti esitatud andmete ülekandmise taotluse täitmisest.

Samas peatükis käsitlesin seejärel ka seda, kas teise isiku õiguste kaitsmisel võib olla lahenduseks see, kui uus vastutav töötleja tugineb teise isiku isikuandmete töötlemisel üldmääruse artikli 6 lg 1 p f kohaselt õigustatud huvile. Õigustatud huvi hindamise testi läbiviimise tulemusena leidsin, et kuivõrd uue vastutava töötleja poolt õigustatud huvile tuginemine toob kaasa uue vastutava töötleja kohustuse teist isikut kui andmesubjekti üldmääruse artikli 14 kohaselt teavitada tema isikuandmete töötlemisest konkreetse vastutava töötleja juures, annab õigustatud huvile tuginemine lõppastmes isikule suurema kontrolli tema isikuandmete töötlemise üle. Isikuandmete töötlemisest teadlikuks saamisel on kolmandal võimalik kasutada üldmäärusest tulenevaid andmesubjekti õigusi uue vastutava töötleja juures. Eelneva põhjal leidis kinnitust magistritöö kolmas hüpotees, et kui andmete ülekandmise õiguse teostamisel kantakse uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed, kaotab kolmas isik oma isikuandmete üle kontrolli ega saa kasutada üldmäärusest tulenevaid andmesubjekti õigusi, välja arvatud juhul, kui uus vastutav töötleja määrab kolmanda isiku isikuandmete töötlemisele õigusliku aluse ja teavitab sellest uut andmesubjekti.

Kokkuvõtlikult omavad töös kinnitust leidnud hüpoteesid positiivset tähendust kolmandate isikute jaoks, kelle isikuandmed võidakse ühes andmesubjekti andmetega uue vastutava töötleja juurde üle kanda. Esiteks tuvastab esimene kinnitust leidnud hüpotees, et andmete ülekandmisel võib esineda riive kolmandate isikute õigusele eraelu puutumatusele ja isikuandmete kaitsele, kui ühes andmesubjekti andmetega kantakse uue vastutava töötleja juurde üle ka kolmanda isiku isikuandmed. Kinnitust leidnud hüpotees teadvustab andmete ülekandmisel tekkida võivaid probleeme ja riivet kolmandate isikute õigustele ja vabadustele. Teise kinnitust leidnud hüpoteesi järgi ei ole vastutaval töötlejal võimalik keelduda kolmanda isiku õiguste ja vabaduste kaitse põhjendusel andmesubjekti esitatud andmete ülekandmise õiguse taotluse täitmisest. Selle hüpoteesi väärtus seisneb selles, et üldmääruses ette nähtud andmesubjekti taotlusest keeldumine ei ole sobiv abinõu kolmandate isikute õiguste ja vabaduste kaitseks.

Kuigi kolmandate isikute isikuandmete ülekandmine uue vastutava töötleja juurde riivab kolmandate isikute õigust eraelu puutumatusele ja isikuandmete kaitsele, leidis käesolev töö kolmandate isikute õiguste kaitse seisukohalt olulise lahenduse. Analüüsist selgus, et kolmanda isiku kontrolli taastamiseks oma isikuandmete üle on ainus üldmäärusest tuvastatav lahendus see, kui uus vastutav töötleja määrab kolmanda isiku isikuandmete töötlemiseks kindlaks õigusliku aluse ning teavitab uut andmesubjekti tema isikuandmete töötlemisest.

RIGHT TO DATA PORTABILITY IN THE GENERAL DATA PROTECTION REGULATION

Abstract

The right to data portability is a completely new concept in European Union data protection law, established in Article 20 of the General Data Protection Regulation (GDPR). It aims to give data subjects more control over their personal data by allowing them to transmit their personal data from one controller to another. Yet, it appears that the right to data portability affects the rights and freedoms of third persons when the data to be transmitted also includes the personal data of a third person.

The purpose of this thesis is to analyse the substance, purpose, prerequisites of the right to data portability, as well as its relation with other rights of data subjects. The controllers' obligations related to the right to data portability were also described. This thesis also focuses on the situation where a data subject wishes to transmit its personal data to another controller, but this data also includes the personal data of third persons. In that regard, this research paper seeked confirmation to three hypotheses. Firstly, the right to data portability interferes the right to privacy and data protection of third persons, when the data to be transmitted under the right to data portability also includes the personal data of third persons. Secondly, the controller cannot refuse to act on the data subject's request to data portability to protect the rights and freedoms of a third person. Thirdly, when the data to be transmitted under the right to data portability also includes the personal data of a third person, the third person loses control over his or her personal data and cannot use the data subjects rights under GDPR, unless the new controller determines a legal basis on processing the personal data of the third person and notifies the third person of processing of his or her personal data.

The method of this research paper is combined of composite, analytic and systematic method. Composite method is used to draw conclusions from relevant court practice. Based on found conclusions, analytic method is used to analyse the possible interference of the rights of third persons. Taking into consideration the substantial volume of GDPR, systematic method is used in order to find appropriate provisions of the GDPR in order to find out whether the hypotheses are confirmed or not.

In the first section, it was found out that the right to data portability, as any other data subject right, can be exercised irrespective of other requests submitted by the same data subject. The main purpose of the right to data portability is to enhance data subject's control over his or her personal data (personal data purpose). In addition to that, the right to data portability also aims

to avoid lock-in of data subjects to one controller and foster economic growth of digital services within the EU (economic purposes).

Prerequisites for exercising the right to data portability include that (i) the processing is based based on consent or contract; (ii) processing is carried out by automated means; (iii) the personal data concerns a specific data subject; (iv) the personal data is submitted by this data subject; and (v) the right to data portability shall not adversely affect the rights and freedoms of others.

In the first section the obligations of controllers were also assessed. The main obligations of the controller are not to hinder portability under Article 20(1), to submit data subject the requested data for free under Article 12(5) and within one month of receipt of the request under Article 12(3). Controllers need not have technically compatible data systems, but they are encouraged to use interoperable formats. Article 29 working party also points out the controller's obligation to ensure that the new controller is acting on behalf of the data subject, yet the GDPR does not establish such obligation. Last but not least, according to Article 12 the controller is obligated to inform data subjects that their personal data is being processed.

When the data is transmitted to another controller, it is appropriate to assess what are the obligations of the new controller. The new controller shall fulfil all obligations as the previous controller, as well as to comply with the principles of data processing under Article 5. It was argued that the new controller shall familiarise itself with the substance of the data that is transmitted to the new controller. When the new controller determines a legal basis to process the personal data of third person (in case such person's personal data is transmitted to the new controller), the controller is obligated to inform third person of data processing.

The first section also addressed the potential security risks of transmitting data from one controller to another. It appeared that the right to data portability poses a risk that someone might act as a data subject to get access to and transmit all the data subject's personal data under the right to data portability. A solution for this is the controllers to adopt an authentication system that requires a data subject, for example, to re-enter its username and password to exercise the right to data portability. What is notable is that the GDPR does not explicitly establish that a controller should identify the person requesting data portability, yet Articles 11, 12 and 32 of the GDPR should be interpreted in a way to recognise the controller's obligation to identify the person requesting data portability.

The second section aimed to find out if the data subject's request to transmit personal data to another controller constitutes an interference with the rights of third persons. Even though the

right to data portability can be exercised only in the existence of five prerequisites at the same time, it is possible that the data to be transmitted can include at the same time the personal data of third persons. For example, when the data subject wishes to transmit contact details of friends, acquaintances or relatives saved in an e-mail service to another controller, or wishes to transmit the payment transaction details from one bank to another. Third persons' rights might also be at stake when the data subject wishes to transmit social media posts to another controller, where the third person is identifiable. When the transmittable data includes the personal data of third persons, it can constitute an interference of third person's right to privacy and data protection.

The right to privacy is protected under Article 7 of the Charter of Fundamental Rights of the European Union (the Charter) and Article 8 of the European Convention on Human Rights, as well as Article 26 of the Constitution of the Republic of Estonia. The right to data protection is guaranteed under Article 8 of the Charter. According to the court practice of Court of Justice of the European Union (CJEU), cases where both interferences of privacy and data protection are in question, an integrated method is used and both rights are assessed together. It is because the CJEU has not differentiated between Articles 7 and 8 of the Charter. It was found that when the data subject requests transmitting data which includes the third person's personal data to another controller, it always interferes with the third person's right to privacy and data protection. The interference is particularly serious when the third person's personal data is disclosed or transferred to determined or undetermined group of people and the third person is unaware of that. It was argued that the purpose of data portability to give data subjects more control over their personal data is a legitimate purpose, whereas the economic purpose and purpose to avoid lock-in of data subjects can not be considered legitimate to limit third person's rights to privacy and data protection. Thus the first hypothesis was confirmed that the right to data portability constitutes an interference of the third person's right to privacy and data portability, if the third person's personal data is being transmitted to another controller when exercising the right to data portability. In order to take into consideration the third person's rights and freedoms, the GDPR should include a provision on how the third perons can exercise control over their personal data that has been transmitted to another controller without their knowledge.

The third section focused on how the GDPR ensures protection of third person's personal data that has been transmitted to another controller under the data subject's request to data portability. It was first analysed whether the criterion of Article 29 working party to extract inferred data or data related to security of system protects the rights and freedoms of the third

person whose personal data has been transmitted to another controller. It was found that this criterion is not suitable to protect the rights and freedoms of third parties, because the personal data of a third person is not considered inferred data or data related to security of system that is subject to extraction.

In the third section I also assessed the controller's right not to act on the request of the data subject in order to protect the third person's rights and freedoms. The controller can refuse to act on the request when the request is manifestly unfounded or excessive, in particular because of their repetitive character. A request is manifestly unfounded when the controller realises at first sight that it is objectively impossible to fulfil such request. A request is excessive in particular when it is repetitively submitted, but taking into consideration that the right to data portability expects controllers to have suitable technical solutions to transmit data, the controller should not refuse to act on the data subject's request on this ground. It was also noted that the controller simply does not become aware if the data to be transmitted includes personal data of third persons, because the GDPR does not obligate the controller to familiarise itself with the data that is transmitted. Thus the second hypothesis of this thesis was confirmed: the controller can not refuse to act on the data subject's request to data portability to protect the rights and freedoms of a third person.

The last part of section three was focused on a possible solution for protecting the rights and freedoms of third persons. It was found that the controller should determine a legal ground to process the personal data of third persons. I conducted a three-stage analysis to assess whether it would be possible for the new controller to rely on legitimate interest under Article 6(1), point f. The result of this analysis showed that the new controller has the legitimate interest to process the personal data of a third person that has been transmitted over to this new controller. A remarkable aspect is that when the new controller determines a legal ground for processing, it shall also notify the third person of his or her personal data being processed pursuant to Article 14. Based on these considerations, the third hypothesis was confirmed that when the data to be transmitted under the right to data portability also includes the personal data of a third person, the third person loses control over his or her personal data and can not use the data subjects rights under GDPR, unless the new controller determines a legal basis on processing the personal data of a third person and notifies the third person of processing of his or her personal data.

As a result, this thesis had a positive outcome on the protection of third persons that might get involved in another data subject's request to data portability. The confirmation of first hypothesis helps to recognise that the right to data portability interferes the third person's rights

to privacy and data protection when the transmittable data includes personal data of third persons. The confirmation of the second hypothesis showed that the controller cannot refuse to act on data subject's request to transmit data to protect the rights and freedoms of third persons. The most important outcome shows that it is possible to protect the rights and freedoms of third persons whose data has been transmitted to another controller without their knowledge. For that end, the controller should determine a legal ground for processing the third person's personal data, preferrably based on legitimate interest, and notify him or her of the processing. Hence the third person becomes aware of the processing of his or her personal data by another controller and can exercise all data subjects' rights under GDPR.

LÜHENDID

AKI – Andmekaitse inspektsioon

EIK – Euroopa Inimõiguste Kohus

EIÕK – Inimõiguste ja põhivabaduste kaitse konventsioon

EK – Euroopa Kohus

ELTL – Euroopa Liidu toimimise leping

Harta – Euroopa Liidu põhiõiguste harta

Üldmäärus – Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)

KASUTATUD ALLIKAD

KASUTATUD KIRJANDUS

1. Alexy, R. Põhiõigused Eesti põhiseaduses. – Justiitsministeeriumi juriidilise ekspertiisi komisjon, 1997.
2. Andmekaitse inspektsioon. Isikuandmete töötleja üldjuhend 19.03.2019. Kättesaadav veebis: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/2019%20juhised/Isikuandmete%20tootleja%20uldjuhend.pdf – 14.04.2019.
3. Artikli 29 alusel asutatud andmekaitse töörühm. Suunised andmete ülekandmise õiguse kohta, kinnitatud Euroopa Andmekaitsenõukogu poolt 05.04.2017. Kättesaadav veebis: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233
4. Data Protection Network. Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation, 06.04.2018. Kättesaadav veebis: https://www.fairtrade.org.uk/~/media/FairtradeUK/Resources%20Library/Data%20Protection%20Network%20-%20Guidance%20on%20the%20use%20of%20legitimate%20interest.pdf – 14.04.2019.
5. De Hert, P., Papakonstantinou, V., Beslay, L., Sanchez, I. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. – Computer Law & Security Review 2018/34, Issue 2.
6. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne 2017. § 26, p 6 (viidatud: M. Ernits. Kommentaar PS §-le 19, p 3.1.2 (koos alapunktidega) väljaandes Ü. Madise jt. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Kolmas, täiendatud väljaanne. Tallinn: Juura, Õigusteabe AS, 2012; R. Alexy. Põhiõigused Eesti põhiseaduses. Juridica 2001, lk 5-96, p 6.1.). Kättesaadav veebis: https://www.pohiseadus.ee/ – 14.04.2019.
7. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne 2017. Kättesaadav veebis: https://www.pohiseadus.ee/ – 14.04.2019.
8. Engels, S., Nordemann, J. B. The Portability Regulation (Regulation (EU) 2017/1128): A Commentary on the Scope and Application. – Journal of Intellectual Property, Information Technology, and Electronic Commerce Law 2018/9.
9. European Commission. Special Eurobarometer 431 „Data Protection“. Publication: June 2015. Kättesaadav veebis: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf – 14.04.2019.

10. European Union Agency for Fundamental Rights and Council of Europe. Handbook on European data protection law 2018 edition. Kättesaadav veebis: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf – 14.04.2019.
11. Feiler, L., Forgó, N., Weigl, M. The EU General Data Protection Regulation (GDPR): A commentary. Globe Law and Business 2018.
12. Graef, I., Husovec, M., Purtova, N. Data Portability and Data Control: Lessons from an Emerging Concept in EU Law. – German Law Journal 2018/19, No. 6.
13. Graef, I. Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union. – Telecommunications Policy 2015/39.
14. Information Commissioner's Office. Guide to the General Data Protection Regulation (GDPR) 2018.
15. Kelleher, D., Murray, K. EU Data Protection Law. Bloomsbury Professional 2018.
16. Lambert, P. B. Understanding the New European Data Protection Rules. Taylor & Francis Group 2018.
17. Lynskey, O. Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order. – International and Comparative Law Quarterly, 2014/63, Issue 3.
18. Maruste, R. Konstitutsionalism ning põhiõiguste ja –vabaduste kaitse. Tallinn: Juura 2004.
19. Oriseg, C. GDPR and Personal Data Protection in the Employment Context. – Labour and Law Issues 2017/3, No 2.
20. Peers, S. jt (koost). The EU Charter of Fundamental Rights: A Commentary. Hart Publishing 2014.
21. Pyykkö, E. Data protection at the cost of economic growth? – European Credit Research Institute Commentary 2012, No 11. Kättesaadav veebis: https://www.ceps.eu/system/files/ECRI%20Commentary%20No%2011%20Data%20protection.pdf
22. Rücker, D. Development and Importance of the Data Protection Reform. – New European General Data Portection Regulation: A Practitioner's Guide. Nomos Verlagsgesellschaft, Baden-Baden 2018.
23. Schrey, J. General conditions for data processing in companies under the GDPR. – Rücker, D., Kugler, T. New European General Data Protection Regulation: A Practitioner's Guide. Nomos Verlagsgesellschaft, Baden-Baden 2018.
24. Swire, P., Lagos, Y. Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. – Maryland Law Review 2013/72, Issue 2.

25. Tupay, P. K. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. – Juridica 2016/IV.
26. Tupay, P. K. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. – Juridica 2016/IV (viidatud: Saksamaa Liitvabariigi andmekaitse ja informatsioonivabaduse inspektroni Andrea Voßhoffi seisukoht, lk 1 jj; Austria andmekaitseeksperdi Waltraud Kotschy arvamus; Kasseli Ülikooli professori Alexander Roßnageli seisukoht).
27. Van den Auwermeulen, B. How to attribute the right to data portability in Europe: A comparative analysis of legislations. – Computer Law & Security Review 2017/33.
28. Van den Auwermeulen, B. How to attribute the right to data portability in Europe: A comparative analysis of legislations. – Computer Law & Security Review 2017/33 (viidatud: De Graef, I., Verschakelen, J., Valcke, P. Putting the right to data portability into a competition law perspective. (2013) Annual review, The Journal of the Higher School of Economics 53, 58).
29. Vanberg, A. D., Ünver, M. B. The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? – European Journal of Law and Technology 2017/8, No 1. Kättesaadav veebis: http://ejlt.org/article/view/546/726#_ftnref4
30. Velbri, S. Isikuandmete kaitse üldmäärusest tulenev nõusoleku vajadus ja selle tingimused isikuandmete töötlemisel äriühingute poolt. Magistritöö. Tallinn: Tartu ülikooli õigusteaduskond 2018.
31. Voigt, P., Von dem Bussche, A. The EU General Data Protection Regulation (GDPR): A practical guide. Springer International Publishing AG 2017.
32. Voigt, P., Von dem Bussche, A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing AG 2017 (viidatud: Kamlah, in: Plath, BDSG/DSGVO, Art. 12 (2016), rec. 20).
33. Voigt, P., Von dem Bussche, A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing AG 2017 (viidatud: Example drawn from Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 21).

KASUTATUD ÕIGUSAKTID

34. Avaliku teenistuse seadus. – RT I, 13.03.2019, 37.
35. Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
36. Euroopa Liidu põhiõiguste harta. – ELT 2012/C 326/02.

37. Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EÜT L 281, 23.11.1995, lk 31-50.
38. Euroopa Parlamendi ja nõukogu direktiiv 2002/21/EÜ, 7. märts 2002, elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv). – EÜT L 108, 24.4.2002, lk 33—50 (eestikeelne eriväljaanne: ptk 13, kd 029, lk 349 – 366).
39. Euroopa Parlamendi ja nõukogu direktiiv 2002/22/EÜ, 7. märts 2002, universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul (universaalteenuse direktiiv). – EÜT L 108, 24.4.2002, lk 51—77 (eestikeelne eriväljaanne: ptk 13, kd 029, lk 367 – 393).
40. Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119/1, 04.05.2016, lk 1–88.
41. Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II, 2000, 11, 57.
42. Lissaboni leping. – ELT 2007/C 306/01.

KASUTATUD KOHTUPRAKTIKA

Riigikohtu praktika

43. RKHKo 3-3-1-3-12.

Euroopa Kohtu praktika

44. EKo C-28/08 P, *Euroopa Komisjon vs The Bavarian Lager Co. Ltd*.
45. EKo C-418/11, *Texdata Software*, p 84 (viidatud: EKo C-28/05, *Dokter*, p 75 ja ühendatud kohtuasju EKo C-317/08 ja C-320/08, *Alassini* p 63).
46. EKo C-58/08, *Vodafone* jt.
47. EKo C-73/07, *Satakunnan Markkinapörssi ja Satamedia*.
48. EKo C-92/09, *Volker und Markus Schecke*, p 48 (viidatud: EKo C-112/00, *Schmidberger*, p 80 ja seal viidatud kohtupraktika).
49. EKo liidetud kohtuasjades C-293/12 ja C-594/12, *Digital Rights Ireland Ltd. v Iirimaa*.
50. EKo liidetud kohtuasjades C-465/00, C-138/01 ja C-139/01, *Österreichischer Rundfunk*.
51. EKo liidetud kohtuasjades C-92/09 ja C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert vs Land Hessen.*

52. EKo ühendatud kohtuasjades C-468/10 ja C-469/10. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) vs. Administración del Estado.*

Euroopa Inimõiguste Kohtu praktika

53. EIKo 13710/88 *Niemietz vs Germany*.
54. EIKo 253/07, *Copland vs United Kingdom*.
55. EIKo 25390/94, *Rekvényi vs. Ungari*.
56. EIKo 27798/95, *Amann vs. Šveits*.
57. EIKo 30562/04 ja 30566/04, *S. ja Marper vs. Ühendkuningriik*.

Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Kristena Paalmäe

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

„Andmete ülekandmise õigus isikuandmete kaitse üldmääruses“,

mille juhendaja on *dr. iur* Mario Rosentau ja kaasjuhendaja *mag. iur.* Annika Vait,

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.

Tartus, **30.04.2019**