

TARTU ÜLIKOOL  
ÕIGUSTEADUSKOND  
ERAÕIGUSE OSAKOND

Liis Miller

**LEPINGUPOOLTE ÕIGUSTE TASAKAALUSTAMINE KAASAEGSETES  
TÖÖSUHETES ANDMEKAITSE ÜLDMÄÄRUSE KONTEKSTIS**

Magistritöö

Juhendaja  
LLM Mari Männiko

Tallinn  
2018

## SISUKORD

SISSEJUHATUS	3
1. VASTANDUVAD ÕIGUSED TÖÖSUHTES	7
1.1. Töötaja eraelu puutumatus	7
1.2. Isikuandmete kaitse	8
1.3. Ettevõtlusvabadus ja selle sisu	11
2. LEPINGUEELNE PERIOOD	15
2.1. Värbamisel küsitavate isikuandmete töötlemise alused	16
2.2. Kandidaadi isikuandmete kogumine	20
2.3. Kandidaadi isikuandmete säilitamine	28
3. ÕIGUSTE TASAKAALUSTAMINE TÖÖLEPINGU AJAL	32
3.1. Töötaja isikuandmete kogumine	32
3.2. Töötaja isikuandmete avaldamine	35
3.3. Kommunikatsiooni jälgimine ja sõnumisaladuse kaitse	37
3.4. Metaandmed ja privaatsus	41
3.5. Eriliigilised isikuandmed töösuhtes	44
3.6. Kaugtöö	56
3.7. Rahvusvahelised töösuhted	60
KOKKUVÕTE	67
BALANCING THE RIGHTS OF THE PARTIES IN THE CONTEXT OF MODERN EMPLOYMENT AND GENERAL DATA PROTECTION REGULATION. Abstract	71
Kasutatud materjalid	77
Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks	87

## SISSEJUHATUS

Töösuhted on olemuslikult alati keerulised, kuivõrd omavahel on pidevas kollisioonis ühe poole majanduslikud huvid teise poole põhiõiguste ja -vabadustega. Lepinguõiguslikult on tegemist küll poolte võrdsusega, kuid praktikas mõistetakse töölepingulist suhet pigem kui alluvussuhet,<sup>1</sup> kuna tööandjale on oma huvide kaitseks muuhulgas antud ka õigus töötajat ja töö tegemist kontrollida.<sup>2</sup>

Mingil viisil töötamine puudutab väga suurt osa elanikkonnast ning inimesed veedavad tööl märkimisväärse osa oma ajast. Seda silmas pidades on Euroopa Andmekaitseasutuste töögrupp märkinud, et töötajad ei jäta igal hommikul tööle tulles oma eraelu töökoha ukse taha vaid neil on õiguspärane ootus privaatsusele ka töökohas, sest märkimisväärne osa suhetest teiste inimestega seondubki just inimese töökeskkonnaga.<sup>3</sup> Vastav käsitlus põhineb Euroopa Inimõiguste Kohtu (EIKo) lahendil, mille kohaselt hõlmab eraelu hõlmab ka õigust luua ja arendada inimsuhteid ning seda õigust ei tohiks automaatselt välistada ka töö- või ärilistes suhetes, kuivõrd need on paljudele inimestele olulisimaks võimaluseks suhete loomisel ja arendamisel.<sup>4</sup>

Info- ja kommunikatsioonitehnoloogia ning sotsiaalmajanduslike arengute tõttu ühiskonnas on nii töötamine kui töökeskkond teisenenud. Näiteks võimaldatakse klassikalise kellast-kellani kontoritöö kõrval tööd teha ka paindliku graafiku alusel ja kaugteel, mis tähendab seda, et töötaja on oma tegevustes varasemast oluliselt iseseisvam ja sõltumatum. Ühest küljest toetab selline töötajatele üha suuremate vabaduste andmine küll lepingupoolte võrdsuse printsiipi, kuid teisalt nõrgestab see töösuhetele omast tööandja kontrolli põhimõtet,<sup>5</sup> millest tulenevalt võivad tööandja majanduslikud huvid ohus olla.

Olenemata töö iseloomust või selle tegemise kohast toimub töötaja isikuandmete töötlemine töösuhtes paratamatult, seda nii tööandja õigustatud huvi, kui ka tema seadusjärgsete

---

<sup>1</sup> A. Henberg. Isikuandmete töötlemine töösuhtes. - *Juridica* VIII/2005 lk 561

<sup>2</sup> Töölepinguseadus § 28 lg 1 p 11 - RT I 28.12.2017, 43

<sup>3</sup> *Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace*, 29.05.2002, lk 4

<sup>4</sup> EIKo 13710/88 *Niemietz vs Germany* 16.12.1992 p 29

<sup>5</sup> TLS § 1 lg 1

kohustuste täitmise tõttu. Töölepinguseadus (TLS) paneb tööandjale kohustuse austada ja kaitsta töötaja põhiõiguseid,<sup>6</sup> sh ka isikuandmeid, mille tagamiseks kohustab senikehtiv Isikuandmete kaitse seadus (IKS) tööandjal kui vastutaval töötajal kasutusele võtma erinevaid organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid.<sup>7</sup> Käimasolev andmekaitse reform ning 24.05.2018 jõustuv Andmekaitse üldmäärus (edaspidi viidatud kui GDPR)<sup>8</sup> toovad endaga kaasa vastutava töötaja vastutuse andmekaitse nõuete rikkumisel, mis tõsisematel juhtudel võib tähendada suuri rahatrahve. Seega on käesoleval ajal eriti oluline tagada töösuhtes õiguste ja kohustuste tasakaal.

Andmekaitse Inspektsioon (AKI) on 2011. aastal koostanud juhise, milles käsitletakse isikuandmete kaitse töösuhetes. Juhendmaterjali on viimati 2014. aastal täiendatud renditööjõudu puudutava osaga.<sup>9</sup> Arvestades aga käimasolevat andmekaitse reformi ja teisenenud töökeskkonda, vajavad ka AKI suunised täiendust.

Magistritöö põhieesmärk ongi olnud kantud soovist luua vaatlusaluses valdkonnas terviklik käsitus, mis kajastaks töösuhete aktuaalprobleeme nii siseriikliku, kui rahvusvahelise materiaalõiguse võtmes ning hõlbustaks seeläbi töötaja eraelu ja andmekaitse põhimõtete tagamise tasakaalustamist tööandja seadusjärgsete kohustuste ja õigustatud huviga. Sellest tulenevalt on magistritööl ka praktiline väärtus, kuivõrd käsitletud õigusliku raamistiku ja aktuaalprobleemide alusel on tööandjatel võimalik luua või täiendada oma organisatsioonisiseseid regulatsioone ja koolitada või nõustada oma töötajaid.

Käesolevas magistritöös esitab autor hüpoteesi, et teisenenud töökeskkonnas ei ole tööandjal võimalik oma GDPR-st tulenevat vastutava töötaja vastutust sisustada, kuivõrd see takistab tema ettevõtlusvabaduse raames tagatud kontrolliõiguse realiseerimist.

Hüpoteesi kontrollimiseks on töö on jagatud kolme peatükki, millest esimene keskendub põhimõistete ja töösuhete poolte õiguste avamisele läbi kehtiva Eesti õiguse.

---

<sup>6</sup> TLS § 28 lg 1 p 11

<sup>7</sup> Isikuandmete kaitse seadus § 25 – RT I 06.01.2016, 10

<sup>8</sup> Euroopa Parlamendi ja Nõukogu määrus 2016/679 EL füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta. ELT L 119/1

<sup>9</sup> Andmekaitse Inspektsioon (koost.) Isikuandmete töötlemine töösuhetes. Juhendmaterjal 2011

(täiend.23.05.2014). Arvutivõrgus:

[http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/Isikuandmed%20t%C3%B6%20suhetes%20juhendmaterjal26%2005%202014\\_0.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%20suhetes%20juhendmaterjal26%2005%202014_0.pdf) 06.04.2018

Teine peatükk vaatleb poolte kohustusi lepingueelsel perioodil ehk värbamisprotsessis. Keskseteks uurimisküsimusteks on kandidaadi isikuandmete töötlemise õiguslikud alused, isikuandmete kogumise võimalused ning kandideerimismaterjalide säilitamine. Privaatsuse ja andmekaitsealaseid küsimusi vaadeldakse läbi terve värbamisprotsessi, võrreldes kehtivaid eraõiguslikke norme avaliku teenistuse omadega. Kahetsusväärset leiab Eesti kohtupraktikast veel väga vähe kaasuseid, mis vaatlusalust valdkonda ja selles eksisteerivaid probleeme illustreeriks, seetõttu on küsimuste lahendamisel lähtutud eelkõige sotsiaalsetest uuringutest, töölepinguseaduse ja avaliku teenistuse seaduse erinevustest, eriseadustest, Andmekaitse Inspeksiooni nõuannetest ja esitatud võrdlusena ka näiteid välisriikidest.

Kolmas peatükk on oma sisult kõige mahukam, kuivõrd hõlmab endast isikuandmete kaitse temaatika ja privaatsusõiguse töösuhte ajal. Põhilisteks uurimisküsimusteks on töötaja jälgimine ja kommunikatsioonivahendite kontrollimine kaasaegses töökeskkonnas, samuti eriliigiliste isikuandmete töötlemine ning kaugtöötamisel tekkivad õiguste kollisioonid. Teemade lahkamisel on kasutatud asjakohast siseriiklikku ja EIKo praktikat, Andmekaitse Inspeksiooni soovitusi, erialaartikleid ja välisriikide õigust. Samuti on välja toodud töölepinguseaduse ja avaliku teenistuse seaduse erisused.

Magistritöös on kasutatud andmekogumismeetodit ja tõlgendavat meetodit, aga ka analüüsivat ja võrdlevat meetodit. Töös on allikatena kasutatud nii rahvusvahelisi, kui siseriiklikke normatiivmaterjale,<sup>10</sup> erialakirjandust, õigusteadlaste arvamusi, kohtupraktikat, eri ametkondade juhiseid ning soovitusi ja erinevaid teemakohaseid sotsiaalseid uuringuid.

Läbivalt on töös omavahel võrreldud eraõiguslikke töösuhteid reguleerivaid asjakohaseid õigusakte avaliku teenistuse omadega. Teiste riikide näidetena on vaadeldud Soomet, kus on peetud vajalikuks vaatlusalune teema eriseadusega<sup>11</sup> reguleerida ning Ühendkuningriigi

---

<sup>10</sup> Autori märkus: kuivõrd töö kirjutamise ajal oli Isikuandmete kaitse seadus ettevalmistamise faasis, on aluseks võetud 16.04.2018 Isikuandmete kaitse seaduse eelnõu 616 SE ja selle seletuskiri. Kättesaadav: <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/e14c5e2f-b684-4aa4-a7dd-ffb76f63f395/Isikuandmete%20kaitse%20seadus> 18.04.2018

<sup>11</sup> *Laki yksityisyyden suojasta työelämässä* 759/2004. Arvutivõrgus inglisekeelsena: <http://www.finlex.fi/fi/laki/kaannokset/2004/en20040759.pdf> 27.03.2017

andmekaitseasutuse juhendit,<sup>12</sup> mis on küllaltki sarnane Andmekaitse Inspektsiooni asjakohasele ettevõtetetele suunatud soovituslikule juhendile.

Kuivõrd tegemist on teemaga, mis liidab jurisprudentsi info- ja kommunikatsioonitehnoloogiaga, on töös kasutatud ka sellealast kirjandust, uudisartikleid, blogipostitusi ja arvamusi, millel teadusallikana on küll vähene väärtus, kuid mis aitavad käsitletud teemasid ja seisukohti paremini avada ning mõista.

Magistritöö autor avaldab suurimat tänu oma juhendaja, Mari Männikole, kelle loengud äratasid esmase huvi andmekaitse ja privaatsuse vastu ning kelle asjatundlikud kommentaarid ja soovitused olid hindamatuks abiks käesoleva töö valmimisel.

Magistritööd iseloomustavateks märksõnadeks on ettevõtlusvabadus, privaatsusõigus, eraelu, andmekaitse ja tööõigus

---

<sup>12</sup> *United Kingdom Information Commissioner's Office. The Employment Practices Code*, 2011. Arvutivõrgus: [https://ico.org.uk/media/for-organisations/documents/1064/the\\_employment\\_practices\\_code.pdf](https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf) 27.03.2018

# 1. VASTANDUVAD ÕIGUSED TÖÖSUHTES

## 1.1. Töötaja eraelu puutumatus

Põhiseaduses, mis on tugevasti läbipõimitud Euroopa Inimõiguste ja Põhivabaduste Konventsiooni (EIÕK) põhimõtetega, on isikute privaatsust kaitstud mitme erineva sättega - paragrahv 26 näeb ette perekonna- ja eraelu puutumatuse, paragrahv 33 kodu puutumatuse ning 43 annab sõnumisaladuse kaitse.

Perekonnaelu puutumatuse tähtsusest räägib asjaolu, et ka PS § 27 lg 1 annab sellele riigi kaitse. Seejuures tuleb aga silmas pidada, et PS § 26 on sätestatud kvalifitseeritud seadusereservatsiooniga, PS § 27 lg 1 aga ilma seadusereservatsioonita,<sup>13</sup> mis tähendab, et ühel juhul oleks riive perekonnaellu siiski teatud asjaoludel lubatud, teisel juhul on kaitse absoluutne.

Õigusteoorias on asutud seisukohale, et konkureerivate sätete puhul, tuleb valida see, mille kaitse on ulatuslikum.<sup>14</sup> Seega perekonnaelu puutumatust rõhutab PS § 27 lg 1, mis tõrjeõiguslikust positsioonist vaadatuna ei anna mitte üksnes õigust keelata riigi sekkumine pereellu, vaid ka õiguse nõuda riigilt kaitset kolmandate isikute sekkumise eest.

Seega on põhiseaduslikult igäühele tagatud õigus nõuda era- ja perekonnaelu austamist; kodupuutumatust ning sõnumisaladuse kaitset.

Töölepinguseaduses (TLS) on viide töötaja põhiõiguste austamise kohta välja toodud paragrahvi 28 lg 2 p-s 11 – tööandja on kohustatud austama töötaja privaatsust ja kontrollima töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi. Avaliku teenistuse seaduses (ATS) vastav säte puudub. Selline asjaolu tõstatab tahes-tahtmata küsimuse kas ametnikul peaks seetõttu olema väiksem ootus privaatsusele, kui töölepingulisel töötajal?

Ametnike puhul tuleb arvesse võtta, et märkimisväärne osa nende töösuhtest, sh ka

---

<sup>13</sup> K. Jaanimägi, L. Oja. Põhiseaduse § 27 kommentaar p 10 – Ü. Madise (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017. Arvutivõrgus: <http://www.pohiseadus.ee/index.php?sid=1&ptid=32&p=27> 11.04.2018

<sup>14</sup> sama

palgaandmed, ametijuhend ja tööine tegevus üldiselt, on käsitletavad avaliku teabena,<sup>15</sup> mille osas on riigi kodanikel põhiseaduslik teabeõigus (PS § 44 lg 2) ning selgus ja läbipaistvus avaliku võimu tegevuse osas on aga demokraatliku riigi üheks alustalaks.<sup>16</sup>

Seda asjaolu on arvesse võetud ka ATS-is endas, kui 01.04.2013.a jõustunud muudatustega toodi mõiste „ametnik“ kõrvale ka mõiste „töötaja.“<sup>17</sup> Vaheteo tingis käsitlus, mille kohaselt on ametnikud isikud, kes teostavad avalikku võimu, vastutavad teiste isikute üldiste huvide kaitse eest ja mõjutavad isikute põhiõiguseid.<sup>18</sup>

Kuivõrd kõik avalikud teenistujad sellise määratluse alla siiski ei mahtunud, peeti vajalikuks endiste „abiteenistujate“ asemel kasutusele võtta mõiste „töötaja,“<sup>19</sup> kellel iseenest võiks eeltoodust tulenevalt olla seega ka suurem ootus privaatsusele. Muuhulgas toetab vastavat käsitlust ka asjaolu, et erinevalt ametnikest ei kuulu avaliku teenistuse töötajate palgaandmed ja ametijuhendid avalikustamisele. Seega ei tähenda avalikus teenistuses töötamine tingimata alati seda, et isik on olukorras, kus tema eraelu puudutavad andmed (eeskätt sissetulek ja töö sisu) on paratamatult avalik teave. Privaatsuse ulatus sõltub pigem sellest, kas tegemist on ametnikuga, kes teostab avalikku võimu ja kasutab avalikke vahendeid või pelgalt avaliku teenistuse töötajaga, kes täidab riigiasutuses üksnes tugifunktsioone.

## 1.2. Isikuandmete kaitse

Informatsiooniline enesemääramisõigus on põhiseaduses hõlmatud nii paragrahviga 19, mis sedastab üldise vaba eneseteostusõiguse; paragrahviga 42, mis keelab riigiasutustel isiku tahte vastaselt tema veendumuste kohta andmete talletamise ning paragrahviga 44, mis

---

<sup>15</sup> Avaliku teabe seadus (AvTS) § 3 lg 1; § 28 lg 1 p 25 - RT I, 06.01.2016, 7

<sup>16</sup> Andmekaitse Inspeksioon. Avaliku teabe seaduse üldjuhend. Tallinn: 2010. Täiendatud märtsis 2016. lk 27. Arvutivõrgus:

[http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf)  
22.11.2016

<sup>17</sup> Avaliku teenistuse seaduse eelnõu nr 193 SE seletuskiri lk 8. Arvutivõrgus:

<https://www.riigikogu.ee/tegevus/eelnoud/eelnou/c99b9c50-6462-4182-a6ce-d182400e1bae>

<sup>18</sup> C. Demmke. *European Civil Services between Tradition and Reform*. European Institute of Public Administration, Maastricht, Netherlands, 2004, p 100.

<sup>19</sup> K. Lang, I. Pärnamägi, E. Sarapuu. Avaliku teenistuse seaduse käsiraamat. Justiitsministeerium. Tallinn: 2013 lk 33. Arvutivõrgus: [http://www.avalikteenistus.ee/public/Jurgen/avaliku\\_teenistuse\\_seaduse\\_kasiraamat.pdf](http://www.avalikteenistus.ee/public/Jurgen/avaliku_teenistuse_seaduse_kasiraamat.pdf)  
22.11.2016



sätetab üldise informatsiooni saamise õiguse.

Seega on isikul tulenevalt põhiseadusega kaitstavast vabast eneseteostusest üldjuhul võimalik ise otsustada, millist informatsiooni ja millises ulatuses ta enese kohta välja jagab. Riik ega teised isikud ei tohi ilma andmesubjekti nõusolekuta või seadusest tuleneva õigusega tema kohta andmeid koguda ega mis tahes muul viisil töödelda ning samuti on isikul õigus informatsiooni saada, sh teada, milliseid tema andmeid kogutakse ning millisel eesmärgil.

Senikehtiv IKS nägi isikuandmete töötlemise peamise seadusliku alusena ette andmesubjekti nõusoleku (IKS § 10 lg 1) ning haldusorgani puhul juriidilise kohustuse olemasolu (IKS § 10 lg 2). Ilma andmesubjekti nõusolekuta oli töötlemine lubatud, kui vastav kohustus tulenes seadusest; EL-i õigusaktist või muust välislepingust tuleneva juriidilise kohustuse olemasolu korral; andmesubjektiga sõlmitud lepingu täitmiseks või täitmise tagamiseks; või üksijuhtumil andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada (IKS § 14 lg 1).

Soovist liikmesriikides andmekaitseõudeid ühtlustada, võeti 24.05.2016 vastu Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (edaspidi GDPR), mille artikli 4 lg 1 defineerib isikuandmetena igasuguse teabe tuvastatud või tuvastatava füüsilise isiku (andmesubjekti) kohta; tuvastatav isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.

Võrreldes seni kehtinud Isikuandmete kaitse seaduse paragrahvi 4 esimeses lõikes toodud definitsiooniga, mille kohaselt on isikuandmed mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata andmete kujust või vormist, on GDPRi määratlus selgem. Andmete töötlemisel on jätkuvalt seaduslikuks aluseks andmesubjekti nõusolek (GDPR art 6 lg 1a), kuid sisuliselt samale astmele on paigutatud ka olukorrad, mida senikehtiva IKS-i järgi pigem eranditena käsitleti. Seega on määruse alusel andmete töötlemine lubatud ka juhtudel kui töötlemise vajalikkus tuleneb andmesubjektiga sõlmitud lepingu täitmiseks (art 6 lg 1b); kui töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks (art 6 lg 1c); kui

töötlemine on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitseks (art 6 lg 1d); kui töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks (art 6 lg 1e) ning kui andmete 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 (art 6 lg 1f).

Võrreldes varasemaga on seega juurde tulnud vastutava töötleja või kolmanda isiku “õigustatud huvi” kriteerium, mille kohaldamine nõuab aga igakordset proportsionaalsuse analüüsi, sest õigustatud huvile tuginemine on lubatav üksnes siis, kui andmesubjekti põhiõiguseid töötlemisega liigselt ei riivata. GDPRi põhjenduspunktides on välja toodud, et õigustatud huvi võib mh eksisteerida, kui andmesubjekt ja vastutav töötleja on omavahel töösuhtes.<sup>20</sup>

Töölepinguseaduses (TLS) on andmete nõudmine ja avaldamine kaetud paragrahviga 11, mille kohaselt ei või tööandja lepingueelsetel läbirääkimistel või töölepingu sõlmimist muul viisil ette valmistades, sealhulgas töökuulutuses või töövestlusel, nõuda töölesoojalt andmeid, mille vastu tal puudub õigustatud huvi. Muud asjakohased sätted andmekaitse (näiteks konkursil osalenute andmete säilitamise, edastamise ja kustutamise) osas puuduvad, mistõttu tuleb lähtuda GDPR art 6 lg 1a sätestatud andmesubjekti nõusolekust või teistest artiklis 6 toodud alustest. Töösuhetes oleks nendeks eelkõige art 6 lg 1b ehk lepingu täitmise vajadus või 1f ehk tööandja õigustatud huvi.

Õigustatud huvi alusel andmete töötlemise õigus seondub eeskätt just eraõiguslike töösuhetega, mille puhul võib eraldi välja tuua ka dispositiivsuse ja lepinguvabaduse põhimõtted, mille kohaselt võib töösuhtes esineda mõningaid kõrvalekaldeid seadusest ning tööandjal on vabadus oma lepingupartnerit valida. Seda silmas pidades kohustab näiteks Krediitiasutuste seaduse<sup>21</sup> § 49 krediitiasutuste töötajaid tööle asumisel esitama majanduslike huvide deklaratsiooni vastavalt kehtestatud sisekorrale. Samalaadse kohustuse paneb investeerimisühingutele ka Väärtpaberituru seaduse<sup>22</sup> § 82<sup>4</sup>. Viidatud kohustus võib

---

<sup>20</sup> GDPR põhjenduspunkt 47

<sup>21</sup> Krediitiasutuste seadus – RT I 30.12.2017, 31

<sup>22</sup> Väärtpaberituru seadus – RT I 30.12.2017, 43

vastavalt asutuse siseregulatsioonile hõlmata lisaks töötajale ka tema lähikondseid. Esmasilgul tundub selline kohustus olevat vastuolus isikuandmete töötlemise minimaalsuse printsiibiga<sup>23</sup> ning riivab kolmandate isikute informatsioonilist enesemääramisõigust, kuid teisalt vaadatuna tuleb kaitsta ka investeerimisturul osalejaid, et finants- või investeerimisasutuste töötajad ega nende pereliikmed ei kasutaks ära neile tööülesannete käigus teatavaks saanud andmeid (nn *inside trading* juhtumid), seega tuleb tagada teatav õiguste tasakaal. Andmekaitse eesmärgikohasuse printsiipi<sup>24</sup> silmas pidades, tuleb aga krediitiasutustel arvestada, et eelviidatud andmed on kogutud üksnes huvide konflikti ärahoidmise eesmärgil ning neid ei tohiks ilma andmesubjekti sellekohase nõusolekuta kasutada näiteks erinevate finantstoodete pakkumisel.

Avaliku teenistuse seaduses on väga täpselt andmete nõudmise õigus, nõutavate ja avalikustavate andmete hulk ning avaldamise kord reguleeritud.<sup>25</sup> Samuti korraldavad avalikus teenistuses isikuandmete temaatikat asutuste sisekorrad ja -juhendid,<sup>26</sup> mis võimalike riivete ohtu kahtlemata maandavad. Eeltoodust lähtuvalt võib asuda seisukohale, et avalikus teenistuses on isikuandmete kaitse vähemalt formaalselt paremini tagatud kui eraõiguslikes töösuhetes, sest olukord on lepinguosalistele selgem ning kohustuste täitmine sellevõrra ka lihtsam.

Varemkehtinud IKS-i § 25 kohustas vastutavat andmetöötlejat tarvitusele võtma erinevaid organisatsioonilisi, füüsilisi ja infotehnilisi meetmeid isikuandmete kaitseks. GDPR art-iga 24 on see kohustus jäänud samaks, kuid määruse nõuete rikkumise korral on uue IKS §-des 61 jj kehtestatud kordades suuremad trahvid.

### 1.3. Ettevõtlusvabadus ja selle sisu

Õigusteadlane R. Alexy on sedastanud, et põhiõigusliku vaidluse korral on esmatähtis õiguse

---

<sup>23</sup> GDPR art 5 lg 1c

<sup>24</sup> GDPR art 5 lg 1b

<sup>25</sup> ATS §§ 65, 106; AvTS § 28 jj – RT I 04.07.2017, 11; AÜA § 5 – RT I 26.08.2015, 6

<sup>26</sup> Näiteks: Isikuandmete töötlemine Viimsi Vallavalitsuses. Arvutivõrgus:  
<http://www.viimsivald.ee/isikuandmete-tootlemine/> 23.03.2017

kaitseala määratlemine, et „saavutada ratsionaalsuse minimaalne standard.“<sup>27</sup> Arvestades, et ka käesolevas töös kaalutakse läbivalt töötajate põhiõiguseid tööandja õigustega, tuleb seega lähemalt avada ka ettevõtlusvabaduse olemus.

Põhiseaduse §-ga 31 on antud igaühele õigus tegeleda ettevõtlusega. Majandusleksikon defineerib ettevõtlust, kui „igasugust majandustegevust, mille eesmärgiks on tulu saamine kauba tootmise ja teenuse osutamise teel.“<sup>28</sup> Põhiseaduse kommentaarides on ettevõtlusena mõistetud „tegevust, mille eesmärk on üldjuhul tulu saamine kauba tootmisest, müümisest, teenuste osutamisest jne.“<sup>29</sup> Seega võib üldistatult öelda, et ettevõtluse põhiline eesmärk on majandustegevuses kasumi saavutamine. Samuti on kommentaarides rõhutatud, et kuivõrd tegemist on vabadusõigusega, peab sellega kaasas käima ka vabadus otsustada ettevõtlusega seonduvate üksikküsimuste osas.<sup>30</sup> Seda silmas pidanud on A. Mitt sisustanud ettevõtlusvabadust kui „isiku iseseisvat majandustegevust, mille põhisisuks on majanduslike ressursside koordineerimine ja selleks vajaliku majandusorganisatsiooni kujundamine.“<sup>31</sup>

Seega kuna tööandja on ettevõtja, siis on tema peamiseks huviks oma ettevõtte kasumlikkuse tagamine ning talle on tagatud iseseisev otsustusõigus, siis on tööandjal ka vabadus valida omale töötajaid, kes mõistagi peavad olema kõrgete kvalifikatsioonidega, kandma tööandjaga samu väärtuseid ning sobituma ka ülejäänud töötajaskonnaga. Eeltoodust tulenevalt eksisteerib tööandjal oma huvide realiseerimiseks põhjendatud huvi töötajat puudutava informatsiooni osas.

Lisaks üldisele informatsioonile huvitab tööandjat ka see, et töötaja oleks lojaalne. Kui üldises lepinguõiguslikus tähenduses on lojaalsuskohustus lepingu täitmist kindlustav kõrvalkohustus, siis töösuhete puhul on lojaalsus vastastikkuse suhte eelduseks.<sup>32</sup> Sisuliselt on tegemist võlaõigusseaduse §-st 620 tuleneva käsundisaaja lojaalsuskohustusega, mille võib jagada kaheks – tegutsemiskohustuseks ja hoidumiskohustuseks.<sup>33</sup> Näiteks kohustab TLS § 16 lg 1 töötajat täitma oma kohustusi lojaalselt oma teadmiste ja oskuste kohaselt

---

<sup>27</sup> R. Alexy. Põhiõigused Eesti põhiseaduses. *Juridica* 2001 eriväljaanne 2001, lk 33

<sup>28</sup> U. Mereste. Majandusleksikon I. Eesti Entsüklopeediakirjastuse AS 2003, lk 178

<sup>29</sup> S. A. Erlich, A. Henberg, O. Kask. Põhiseaduse kommentaarid §-le 31, p 5

<sup>30</sup> sama

<sup>31</sup> A. Mitt. Ettevõtlusvabaduse õiguslik olemus. *Juridica* VI/2006, lk 387

<sup>32</sup> E.Ojamäe. Töötaja konkurentsikeeld kui lojaalsuskohustus. *Juridica* II/2004, lk 103

<sup>33</sup> K. Kessa. Saladuse hoidmise kohustus ja konkurentsipiirang töösuhetes. *Magistritöö*. Tartu Ülikool. 2013, lk 7

tööandja kasu silmas pidades ning TLS-i §-d 22 ja 23 sedastavad saladuse hoidmise kohustuse ja konkurentsipiirangu.

Oma ettevõtlusvabaduse tagamiseks ja õiguste realiseerimiseks on töölepinguseadusega antud tööandjale kontrolliõigus (TLS § 28 lg 1 p 11), mida on töölepinguseaduse seletuskirjas ühe töösuhte määrava tingimusena välja toodud<sup>34</sup> ning mida eraldi rõhutab ka TLS-i § 1 lg 1 Kuivõrd tegemist on õigusega, mille teostamine võib endast ohtu kujutada töötaja eraelule, on TLS-i § 28 lg 1 p-s 11 eraldi välja toodud, et kontrolli teostamine peab toimuma viisil, mis neid minimaalselt riivab.

Põhiseaduse kommentaarides on selgitatud, et põhiõiguste vastuolude lahendamisel tuleb hinnata vastanduvaid õigushüvesid, konkreetseid asjaolusid ning abistavalt juurde võtta ka proportsionaalsuse põhimõte,<sup>35</sup> mille kohaselt peab iga riive olema põhiseadusega kooskõlas (nn abinõu sobivus), piirang peab olema demokraatlikus ühiskonnas vajalik (abinõu vajalikkus) ning riive ei tohi moonutada piiratavate õiguste ja vabaduste olemust (abinõu mõõdukus).<sup>36</sup>

Riigikohtu praktikas kasutatakse järjekindlalt käsitlust, mille kohaselt „Sobiv on abinõu, mis soodustab piirangu eesmärgi saavutamist. Sobivuse seisukohalt on vaieldamatult ebaproportsionaalne abinõu, mis ühelgi juhul ei soodusta piirangu eesmärgi saavutamist. Sobivuse nõude sisuks on kaitsta isikut avaliku võimu tarbetu sekkumise eest. Abinõu on vajalik, kui eesmärki ei ole võimalik saavutada mõne teise, kuid isikut vähem koormava abinõuga, mis on vähemalt sama efektiivne kui esimene. Abinõu mõõdukuse üle otsustamiseks tuleb kaaluda ühelt poolt põhiõigusse sekkumise ulatust ja intensiivsust ning teiselt poolt piirangu eesmärgi tähtsust. Mida intensiivsem on põhiõiguse riive, seda kaalukamad peavad olema seda õigustavad põhjused.“<sup>37</sup>

Eeltoodust tulenevalt peab ka tööandja arvestama, et ehkki temale on antud õigus töötajat ning töö tegemist kontrollida, tuleb tal kontrollmehhanismide loomisel ja rakendamisel

---

<sup>34</sup> Töölepingu seaduse eelnõu 299 SE seletuskiri lk 7. Arvutivõrgus:  
<https://www.riigikogu.ee/tegevus/eelnoud/eelnou/92c984a5-95ab-8584-38cd-05fc754e99c4/>

<sup>35</sup> M. Ernits. Põhiseaduse kommentaarid II ptk sissejuhatus p 2

<sup>36</sup> Ernits. PS kommentaarid §-le 11 p 2

<sup>37</sup> RKPJKo 17.07.2009, 3-4-1-6-09, p 21; 15.12.2009, 3-4-1-25-09, p 24

igakordselt hinnata, kas tema ettevõtlusvabadus kaalub üle töötaja õiguse eraelule.

## 2. LEPINGUEELNE PERIOOD

Üldjuhul saab iga töösuhe alguse sellest, et tööandja kuulutab välja konkursi teatud ametipositsiooni täitmiseks.<sup>38</sup> Tööandja eesmärgiks on leida võimalikult parim töötaja võimalikult lühikese aja jooksul ja võimalikult väikeste kuludega.

Erinevalt töölepingulistest töötajatest, kelle puhul sätestab konkreetsed nõudmised tööandja ise, on ametnikele kehtestatud rangemad kvalifikatsiooni ning isikuomaduste nõuded.<sup>39</sup> Avaliku teenistuse seaduse (ATS) seletuskiri märgib, et kuna ametnikud teenivad kogu rahvast ning nende pädevuses on ka teiste isikute suhtes võimuvolituste rakendamine, kaasneb sellega erilise usaldussuhte olemasolu. Ametnikud peavad olema usaldusväärsed, ausad ning eetilised ja usaldussuhte rikkumise korral võib nende suhtes rakendada distsiplinaarmenetlust.<sup>40</sup>

Kui suuremates ettevõtetes/ asutustes on olemas vastava koolituse saanud personalispetsialistid, kes kogu värbamisprotsessi, töölepingute sõlmimise ja muu töökorraldusliku asjaajamise oma õlgadele võtavad, siis enamikes väike- ja mikroettevõtetes kannavad lõviosa ülesannetest tööandjad ise, kes ei pruugi alati olla piisavate teadmistega, tagamaks oma töötajate privaatsuse igakülgse kaitse ning täitmaks seeläbi ka enda kui vastutava andmetöötleja kohustused.

2014. aastal viisid Tartu Ülikooli teadlased eestlaste seas läbi privaatsust käsitleva uuringu, millest muuhulgas selgus, et 41 protsenti vastanutest peab muret isikuandmete kaitstuse pärast ületähtsustatuks.<sup>41</sup> Magistritöö autori hinnangul ei oska inimesed näha probleemi mastaape, kuna infot antakse välja üsna väikestes kildudes ja see tundub neile sellisena vähetähtis. Ka uuringu üks läbiviijatest, Tartu ülikooli sotsiaalmeedia lektor, Maria Murumaa-Mengel, arvab, et sageli ei saa inimesed täpselt aru, mida nende andmetega tehakse

<sup>38</sup> Autori märkus: kui eraõiguslikes töösuhetes on ametikoha täitmine lubatud ka väljaspool konkursi, siis avalikus teenistuses on konkursi korraldamine kohustuslik – Avaliku teenistuse seaduse § 16 lg 1

<sup>39</sup> Nt ATS § 10 lg 1 p-d 1,2.

<sup>40</sup> Avaliku teenistuse seaduse eelnõu 193 SE seletuskiri lk 8. Arvutivõrgus:

<https://www.riigikogu.ee/tegevus/eelnoud/eelnou/c99b9c50-6462-4182-a6ce-d182400e1bae>

<sup>41</sup> K. Nyman Metcalf. Privaatsusõigus inimõigusena ja igapäevatehnoloogiad. Uuringu kokkuvõte. Tartu Ülikooli Ühiskonnateaduste Instituut ja Eesti Inimõiguste Instituut 2014. lk 4. Arvutivõrgus:

<http://www.humanrightsestonia.ee/uuringud-uurimused/privaatsus-inimõigusena-ja-igapaevatehnoloogiad/>  
14.03.2017

ning seetõttu ütlevadki üsna kergekäeliselt, et nad ei hooligi sellest.<sup>42</sup>

Alljärgnevalt käsitletakse värbamisprotsessis enamlevinud probleemseid olukordi ning püütakse neile leida asjakohased ja õiguspärased lahendused, mis arvestavad mõlema poole õiguste ja kohustustega.

## 2.1. Värbamisel küsitavate isikuandmete töötlemise alused

Andmete kogumine mistahes viisil on andmete töötlemine GDPR art 4 lg 2 tähenduses, mis omakorda tähendab, et töötlemine peab toimuma seaduse alusel ning selles sätestatud korras. Kui võrd pooled ei ole omavahel (veel) töölepingulises suhtes ning sellest tulenevalt ei saa andmeid töödelda GDPR art 6 lg 1b alusel, saab uue võimaliku töötaja isikuandmeid koguda üksnes andmesubjekti nõusolekul ehk art 6 lg 1a alusel. Siiski võib teatud ametikohtade puhul eriseadustest tulla tööandjale õigus või kohustus kandidaadi andmete kogumine ka ilma andmesubjekti vastava nõusolekuta art 6 lg 1c alusel (näiteks karistusregistri andmed turvatöötajate, pangatellerite ja ametnike<sup>43</sup> puhul).<sup>44</sup> GDPR art 14 kohustab tööandjaid sellisel juhul aga isikuid ka sellisest andmete kogumisest teavitama.

Soome asjakohases seaduses on samad põhimõtted *expressis verbis* välja toodud, rõhutades nii individuaalse osaluse esmatähtsust, kui iseseisvalt kogutavate andmete puhul (karistusregistri väljavõte) kogumisest teavitamisest.<sup>45</sup>

Võttes arvesse andmetöötamise põhiprintsiipe,<sup>46</sup> tuleb tööandjal igakordselt hinnata, milliseid andmeid, millises ulatuses ta oma eesmärkide saavutamiseks vajab. Seejuures sätestab TLS § 11 tööandja jaoks väga konkreetse piirangu, mille kohaselt ei või tööandja lepingueelsetel läbirääkimistel või töölepingu sõlmimist muul viisil ette valmistades, sealhulgas töökuulutuses või töövestlusel, nõuda töölesooijalt andmeid, mille vastu tal puudub

---

<sup>42</sup> M. Himma. Uuring - Eesti elanikud usaldavad kergekäeliselt oma privaatsaid andmeid erinevatele institutsioonidele. ERR/Novaator. 20.10.2015.

<sup>43</sup> ATS § 15 p-d 1-3

<sup>44</sup> AKI juhendmaterjal lk 24

<sup>45</sup> *Laki yksityisyyden suojasta työelämässä* § 2 lg 4

<sup>46</sup> GDPR art 5



õigustatud huvi. Tööandja õigustatud huvi puudumist eeldatakse eelkõige küsimuste puhul, mis puudutavad ebaproportsionaalselt töölesoojija eraelu või mis ei ole seotud sobivusega pakutavale töökohale (TLS § 11 lg 2). Ka VÕS § 14 lg 2 kohustab lepingupooli teineteist teavitama üksnes neist asjaoludest, mille vastu on teisel poolel, arvestades lepingu eesmärki, äratuntav ja oluline huvi.

Ametnike puhul on olukord veidi piiratum, sest ATS sätestab eraldi nõudeid, millele tulevane ametnik peab vastama,<sup>47</sup> millele omakorda lisanduvad spetsiaalsed hariduse- ja kvalifikatsiooninõuded konkreetset ametikohta silmas pidades. Siiski eksisteerib andmete minimaalsuse ja eesmärgikohasuse printsiip ka avalik-õiguslikes töösuhetes ning ka asutus ei või ametniku kandidaadilt nõuda rohkem andmeid, kui mõistlikult võttes on vajalik.

Ühendkuningriigi andmekaitseasutuse poolt koostatud juhendis viidatakse mõistetele kinnitamine (ingl. k *verification*), mis sisuliselt tähendab kandidaadi avalduse ja selles sisalduva informatsiooni vastavuse kontrollimist tööpakkuja nõuetega ja kontrollimine (ingl.k *vetting*), mis tähendabki juba laiemat taustakontrolli kandidaadi suhtes, sh soovitajatega suhtlemist.<sup>48</sup> Samuti rõhutatakse eelmainitud juhendis individuaalse osaluse põhimõtet ning soovitatakse esmase andmeallikana kasutada andmesubjekti ennast ning alles seejärel vajadusel kontrollima kandidaadi tausta muudest allikatest.<sup>49</sup>

IKT arengut ning eelkõige sotsiaalmeedia võimalusi silmas pidades avaldas juunis 2017 Euroopa Andmekaitseametnike töögrupp uued, eeskätt tööandjatele suunatud juhised, milles muuhulgas toodi välja, et tööandjad ei tohiks värbamisel koguda töölesoojija kohta andmeid tema sotsiaalmeedia kontolt, isegi kui see on avalikult kättesaadav. Samuti on töögrupi hinnangul täielikult taunitav töölesoojijale „sõbrakutse“ saatmine eesmärgiga veelgi rohkem andmeid näha. Juhul, kui tööandja on siiski andmeid sotsiaalmeedia kaudu hankinud, peab ta sellest töölesoovijat teavitama.<sup>50</sup>

Praktilisest küljest on tänases infoühiskonnas sotsiaalmeedia mõju võimatu eirata. Ühelt poolt võib selline andmete kogumise viis olla küll küsitav ning hilisemas vaidluses tuleb tööandjal

---

<sup>47</sup> ATS § 14

<sup>48</sup> *Information Commissioner's Office. The Employment Practices Code*, 2011. lk 14

<sup>49</sup> sama lk 23

<sup>50</sup> *Article 29 Data Protection Working Party. Opinion 2/2017 on data processing at work*. 08.06.2017, lk 11

välja tuua õigustatud huvi sotsiaalmeedia kasutamiseks, kuid samas ei saa ka mööda vaadata üldisele informatsiooni saamise õigusele ning asjaolule, et kui isik on loonud omale avaliku profiili mõnda sotsiaalmeediakeskkonda, siis on ta vaikimisi lubanud oma andmeid ka avalikult kuvada. See, millise jalajälje igäüks endast maha jätab, on aga subjektiivsete valikute küsimus, mida õiguslikult reguleerida ei saa, pigem võiks selles valdkonnas olla fookus suunatud üldisele teavitustööle. Seega ei saa tööandjale mõistlikult võttes ette heita seda, et ta töölesoovija kohta infot ammutab ka viimase avalikult kättesaadavalt sotsiaalmeediakontolt.<sup>51</sup>

Tööandja õigustatud huvi kandidaadi suhtes on hinnanguline kriteerium. Andmekaitse Inspektsiooni seisukohalt tuleb arvestada nii töösuhtet ennast kui konkreetse ametikoha nõudeid.<sup>52</sup> Töölepinguseaduse seletuskiri avaldab kahetsusväärset, et praktikas on liigagi levinud olukorrad, kus tööandja tunneb huvi töötaja eraeluliste andmete, sh nii olemasolevate laste vanuse, kui pereplaneerimise kohta, eesmärgiga leida maksimaalselt tööülesannete täitmisele keskendunud töötaja.<sup>53</sup> Samas on rõhutatud, et sellist informatsiooni ei saa aga värbamisel kasutada ilma, et see viiks ebavõrdse kohtlemiseni, seega võib väita, et tööandjal puudub liigsete eraelu puudutavate küsimuste osas õigustatud huvi,<sup>54</sup> kuivõrd need puudutavad ebaproportsionaalselt kandidaadi eraelu või ei ole kuidagi seotud sobivusega pakutavale töökohale.<sup>55</sup>

Andmekaitse Inspektsioon soovib tööandjatel siiski kõikide kogutavate andmete puhul veelkord endalt küsida, „kas andmed on ikka tõesti valiku tegemisel vajalikud ning kas just sellises ulatuses.“<sup>56</sup> Vastavalt Euroopa Andmekaitseasutuste töögrupi seisukohale ei ole töösuhtes tööandja kohustuste täitmiseks vajalike andmete kogumine juba kandideerimisfaasis õigustatud, värbamise protsessis saab olla õigustatud huvi ainult selliste asjaolude vastu, mille põhjal tehakse tööle värbamise otsus.<sup>57</sup>

Kuigi vastavat selgesõnalist kohustust ei sisaldu TLS-is, tuleb tööandjal järgida ka võrdse

---

<sup>51</sup> Vt ka käesolevas töös edasi lk 24

<sup>52</sup> AKI juhendmaterjal lk 25

<sup>53</sup> TLS seletuskiri lk 21

<sup>54</sup> sama

<sup>55</sup> sama lk 22

<sup>56</sup> AKI juhendmaterjal lk 26

<sup>57</sup> *Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context.* lk 7

kohtlemise põhimõtteid ja diskrimineerimise keeldu juba töökuulutuse vormistamisel. Näiteks on võrdse kohtlemise seaduse (VõrdKS) § 2 lg 1 p 1 ja lg 2 p 1 kohaselt keelatud isikute diskrimineerimine vanuse või seksuaalse sättumuse tõttu töö saamise tingimuste kehtestamisel, sealhulgas värbamis- ja valikukriteeriumide kehtestamisel. VõrdKS § 9 lg 2 lubab erandina töö valdkonnas vanuse alusel isikuid erinevalt kohelda, kui sellel on objektiivne ja mõistlik tööhõivepoliitikat või tööturgu hõlmav õiguspärane eesmärk ning selle eesmärgi saavutamise vahendid on asjakohased ja vajalikud. VõrdKS § 10 lg 1 lubab erandina töö valdkonnas vanuse (või muu seaduses nimetatud tunnuse alusel) isikuid erinevalt kohelda, kui vanus (või muu tunnus) on oluline ja määrav kutsenõue, mis tuleneb kutsetegevuse laadist või sellega seotud tingimustest ning nõude eesmärk on õiguspärane ja nõue proportsionaalne.

Soolise võrdõiguslikkuse seaduse (SoVS) § 8 keelab töö- ja koolituspakkumised, mis on suunatud üksnes ühest soost isikutele. SoVS § 5 lg 2 p 4 lubab erandina tööle saamiseks või koolituse võimaldamisel soo alusel isikuid erinevalt kohelda, kui sugu on teatud kutsetegevuse olemuse või sellega liituvate tingimuste tõttu oluline ja määrav nõue ning taolise erineva kohtlemise eesmärk on õigustatud ja nõue proportsionaalne eesmärgiga.

Ametnike puhul sätestab ATS § 18 lg 1 ühemõtteliselt, et nii värbamine, kui valik peavad põhinema eelnevalt avalikustatud tingimustel ning kandidaatide võrdsel kohtlemisel.

2015. aastal tõdes toonane võrdõigusvolinik Mari-Liis Sepper, et sooliste filtrite kasutamine värbamisel on tänane reaalsus, mis ilmselt ka lähiaastatel veel kuhugi ei kao ning taunis töövestluse käigus kandidaadilt isiklike andmete küsimist. Diskrimineerimise vähendamiseks käis voliniku büroo välja ka idee anonüümse värbamiskeskonna loomisest, milles fookus oleks suunatud üksnes isiku teadmistele, oskustele ja kogemustele.<sup>58</sup>

2017. aastal tekkis klassikaliste tööotsinguportaalide kõrvale Eesti idufirma MeeFrank OÜ loodud mobiilseadme rakendus Frank,<sup>59</sup> mis on eeskätt suunatud IT-ettevõtetele. Sisuliselt on Franki ülesanne omavahel kokku viia talent ja tööpakkuja, kuid seejuures ei ole tööotsijal

---

<sup>58</sup> M. Nael (toim). Sepper: sooline diskrimineerimine töölevõtmisel ei kao ka lähiaastail. ERR. 17.02.2015. Kättesaadav: <http://www.err.ee/530010/sepper-sooline-diskrimineerimine-tolevotmisel-ei-ka-ka-lahiaastail> 20.04.2017

<sup>59</sup> Ettevõtte veebileht kättesaadav: <https://meetfrank.com/> 11.10.2017

vaja sisestada lugematul hulgal andmeid, vaid piisab üksnes nimest, töövaldkonnast, kogemuse pikkusest, praegusest töötasust ning ootustest. Nendele kriteeriumitele vastava tööpakkumise leides, viib Frank pooled kokku ning edaspidine täiendav andmevahetus on juba asjaosaliste enda otsustada. Anonüümsusele rõhub ka teine tööotsinguportaal Talentest, mis samuti keskendub töötaja oskustele ning millega on liitnud mitmed mainekad ettevõtted.<sup>60</sup> Seega on märgata tendentsi, et teatud valdkondades otsitakse ja väärtustatakse pigem oskusi, teadmisi ja kogemusi, kui töötaja selliseid tunnuseid, mille olemasolu või puudumine mitte mingil viisil töösuhet ei mõjuta.

## 2.2. Kandidaadi isikuandmete kogumine

Tulenevalt eelnevast alapeatükist on värbamisprotsessis kandidaadi andmete kogumine lubatud üldjuhul üksnes andmesubjekti enda nõusolekul (GDPR art 4 lg 2). Valdav osa töökuulutustest on avalikud ning kandideerimine on lubatud kõigile, kes oma hinnangul kuulutuses sedastatud kriteeriumitele vastavad. Enamasti on konkurss korraldatud läbi vastava tööotsinguportali (CV Online, CV Keskus, Ekspressjob jms), seega saab sellisel juhul tõsikindlalt väita, et kandidaat tegutseb omal vabal tahtel ning eesmärgipäraselt. Siiski võib ka vabal tahtel antud nõusolek teinekord anda ootamatu tagasilöögi.

### 2.2.1. Töövahendusportaalid

Eesti üks suurimaid nn klassikalisi tööportale, CV Online, võimaldab seadistada töötajatel oma CV kättesaadavust, muutes see kas aktiivseks või passiivseks. Täiendavalt saab kasutaja seadistada CV nähtavust ka teatud ettevõtete järgi, välistades näiteks täielikult teatud ettevõtted.

Töövõtjatele pakub portaal ühe võimalusena teenust, mis võimaldab isikute aktiivsete CV-de vaatamist/ otsimist teatud kriteeriumite alusel (näiteks märksõnaga “jurist”). Seeläbi on tööandja valikuvõimalused suuremad, kuivõrd tööandja kätte jõuavad ka selliste isikute CV-d, kes avaldatud töökonkursil võib-olla ei kandideeriksi.

---

<sup>60</sup> Ettevõtte veebileht kättesaadav: <https://talentest.ee/about> 09.01.2018

Senikehtiva IKS-i kohaselt tuleb andmesubjektile enne tema andmete töötlemist küsida nõusolekut, seejuures on nõusoleku küsimisel rõhutatud andmesubjekti vaba taht, kogutavate andmete koosseisu väljatoomist ning seda, et nõusoleku küsimisel tuleb andmesubjektile teada anda andmetöötaja kontaktandmed, teavitada andmesubjekti andmete kogumise eesmärgist ning ka nende isikute ringist, kellele andmeid võidakse edastada, edastamise tingimused ning andmesubjekti õigused sellise edasise andmetöötluse korral (IKS § 12 lg 1 ja 3). Nõusolekule on kehtestatud kirjalikku taasesitamist võimaldav vorm, vaikimist või tegevusetust nõusoleku andmiseks ei loeta (IKS § 12 lg 2). Andmesubjektile on õigus nõusolek igal ajal tagasi võtta, kuid sellel ei ole tagasiulatuvat jõudu (IKS § 12 lg 7).

GDPR art 4 lg 11 defineerib andmesubjekti nõusolekuna vabatahtlikku, konkreetset, teadlikku ja ühemõttelist tahteavaldust, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate andmete töötlemisega. Seejuures täpsustab art 7 lg 1, et nõusolekul põhineva andmetöötluse korral lasub vastutajal töötlejal kohustus andmesubjekti poolt antud nõusolekut tõendada. Art 7 lg 2 näeb ette, et kui nõusolek antakse kirjaliku kinnitusega, peab see olema muudest küsimustest selgelt eristatud ning esitatud arusaadaval, lihtsasti kättesaadaval kujul, kasutades selget ja lihtsat keelt. Art 7 lg 3 alusel on andmesubjektile õigus nõusolek igal ajal tagasi võtta ning ka see peab olema korraldatud sama lihtsalt kui nõusoleku andmine.

Andmesubjektile nõusoleku küsimisele tuleb edaspidi kohaldada GDPR-ist tulenevaid nõudeid, seejuures kohustub vastutav töötaja ühes nõusoleku küsimisega andmesubjektile ka teatavaks tegema hulga töötlemist puudutavaid andmeid (GDPR art 13). Selles osas on uus IKS sedastanud loetelu informatsioonist, mida vastutav töötaja kohustub andmesubjektile tema andmete töötlemise korral esitama. Lisaks juba eelmainitud andmetele vastutava töötaja kontaktide, andmete töötlemise eesmärgi ning võimalike kolmandate isikute kontaktide, kellele võidakse andmeid edastada tuleb andmesubjektile lihtsalt kättesaadavaks teha ka andmekaitseinspektori ning Andmekaitse Inspektsiooni kontaktid andmesubjekti õiguste rikkumise puhuks (IKS § 21). IKS-i seletuskirja kohaselt peaks selline teave andmesubjektile andma hea ülevaate tema andmete kogumise eesmärgist ning ka tema

õigustest andmete töötlemisel.<sup>61</sup>

CV Online kasutustingimustes on välja toodud, et CV-Online töötleb kasutaja poolt portaalis registreerumisel esitatud ja andmebaasi sisestatud kasutaja isikuandmeid kasutajale teenuste osutamise eesmärgil. CV-Online töötleb kasutaja isikuandmeid ise ning edastab neid andmete saajatele viimastega sõlmitud lepingute täitmiseks. Kasutajal on igal ajal õigus teada saada, milliseid kasutaja isikuandmeid CV-Online töötleb, samuti nõuda kõikide või mõnede isikuandmete töötlemise lõpetamist.<sup>62</sup>

Seega registreerudes CV-Online kasutajaks, annab isik nõusoleku oma andmete töötlemiseks mitte ainult portaalile, vaid ka määramata ringile kolmandatest isikutest kasutajatele, kes läbi portaali omale töötajaid otsivad. Käesoleva magistritöö kirjutamise seisuga ei olnud CV-Online oma kasutustingimusi GDPR-iga vastavusse viinud, seega puudub tööotsijast andmesubjektil tegelikult ülevaade, kellele tema andmeid edastatakse. Ehkki kasutustingimused võimaldavad GDPR art 7 lg-st 3 tulenevat õigust nõusolek andmete töötlemiseks igal ajal tagasi võtta, peab arvestama, et nõusoleku tagasivõtmisel ei ole retrospektiivset jõudu, mis omakorda tähendab, et selleks ajaks kui nõusolek on tagasi võetud, võivad tööotsija andmed olla sattunud juba kümnete kolmandast isikust tööpakkujate kätte, seega sisuliselt puudub andmesubjektil igasugune kontroll oma andmete üle.

CV Online tööpakkujatele mõeldud kasutustingimustes sisalduvad küll kohustus töödelda andmebaasis olevate isikuandmeid vastavalt seadusele, kohustus hoida andmebaasis olevaid isikuandmeid konfidentsiaalsetena ning kasutada neid üksnes eesmärgipäraselt,<sup>63</sup> kuid faktiliselt puudub ka portaalil endal, kui vastutaval töötlejal<sup>64</sup> igasugune kontroll selle üle, mida tegelikult andmetega tehakse ning kuhu neid edastatakse. Seega ei olegi tänases situatsioonis portaalil, kui vastutaval andmetöötlejal, võimalik oma GDPR-ist tulenevaid kohustusi nõuetekohaselt täita.

Ühelt poolt on CV-sse lisatavate andmete hulga kontrollimine mõistagi isikute enda võimuses, kuid tuleb tahes-tahtmata tunnistada, et tööandjate silmis on oluliselt atraktiivsem

---

<sup>61</sup> IKS 16.04.2018 eelnõu 616 SE seletuskiri lk 27

<sup>62</sup> CV Online kasutustingimused tööotsijale p. 3.2. Arvutivõrgus: <http://www.cv.ee/terms/seeker/> 11.04..2018

<sup>63</sup> CV Online kasutustingimused tööpakkujale p. 2.11. Arvutivõrgus: <http://www.cv.ee/terms/client/> 11.04.2018

<sup>64</sup> GDPR art 4 lg 7

põhjalik elulookäsitlus, kui pelgalt faktikogum. Näiteks on mitmed Eesti personalijuhid avaldanud, et mida sisukam CV, seda parem ning tunnistanud, et vähest infot sisaldavatesse avaldustesse väga ei süübitagi.<sup>65</sup> Seega ei saa magistritöö autori hinnangul riskikoormist panna täielikult isikute enda õlule, sest tööotsinguportaali eesmärki silmas pidades, on isikud siiski teatud sundseisus oma andmete avaldamise (mahu) osas. Mõistlikult võttes puudub ka portaalil võimalus takistada isikuandmete levitamist, sest nii töötajad ise, kui ka tööpakkujad prindivad CV-sid välja, jagavad tuttavatega, unustavad neid kergesti kättesaadavatesse kohtadesse jne ning sellise inimfaktori ohjamine ei ole portaalil võimuses ega saagi olla. Kuna töötajad ise muutuvad oma õigustest järjest teadlikumaks, siis ehk asenduvadki CV-Online'i taolised töövahendusportaalid tulevikus anonüümsete talendiotsingu äppidega nagu MeetFrank ja Talentest, kus isikuandmete osas ei kehti põhimõte „rohkem on uhkem“ ning mida on sellest tulenevalt ka lihtsam hallata.

## 2.2.2. Avalike andmete töötlemine

Olenevalt ettevõttest/ asutusest ja töökoha eripäradest on tööandjatel võimalik kandidaadi kohta andmeid koguda nii avalikest kui mitteavalikest kanalitest.

GDPR-i art 6 tähenduses võivad andmed olla avalikud kas seetõttu, et andmesubjekt on andmed ise avalikuks teinud (lg 1a) või nõuab andmete avalikustamist vastutava töötleja juriidiline kohustus (lg 1c) või on avalikustamine vajalik avalikes huvide või avaliku võimu teostamiseks (lg 1e). Eeltoodust lähtuvalt loetakse avalikeks andmeteks muuhulgas ligipääsetavaid sotsiaalmeedia postitusi, pildialbumeid, ilma erilise pingutuseta tuvastatavaid internetikommentaare<sup>66</sup> jms. Samuti ka ajakirjanduses avaldatud tekstid (nt arvamused).<sup>67</sup> Juriidilise kohustuse täitmiseks või avaliku võimu teostamiseks vajalikud avalikustatud andmed on nt erinevate riiklike registrite andmed (rahvastikuregister, karistusregister, kinnistusraamat, abieluvararegister jne), kohtulahendid ja muud andmebaasid (nt ETIS).

---

<sup>65</sup> R. Resmeldt Uusen. Eesti personalijuhid paljastavad: kümme elulist trikki, kuidas kandideerides edumaa saavutada. - Postimees. 20.02.2017

<sup>66</sup> Autori märkus: Mitmed meediaväljaanded võimaldavad artikleid kommenteerida kas anonüümselt või registreeritult. Registreeritud konto on enamjaolt seotud mõne sotsiaalmeedia profiiliga, seega on isiku tuvastamine lihtne. Käesolevalt ei ole mõeldud IP-aadressi abil isiku tuvastamist, mis on omaette protsess ja mida üldjuhul tavatöökohale kandideerides läbi ei viida.

<sup>67</sup> AKI juhendmaterjal lk 31

Nagu töös varasemalt selgitatud, on isiku *googeldamine* iseenesest õiguspärane tegevus, kuid vastavalt GDPR art 14 lg-le 1 tuleb sellisel viisil andmete kogumisel töölesoovijat teavitada andmete kogumise faktist, kogutud andmete koosseisust ning allikatest.

Ühe avaliku andmeallikana saab käesoleval ajal kahtlemata eraldi välja tuua ka sotsiaalmeedia (Facebook, Instagram, Twitter, LinkedIn jms). Katriin Visamaa oma bakalaureusetöös välja toonud, et kui LinkedIn on värbajate seas peamiselt kasutatav *head-hunting*'u eesmärgil, siis Facebook leiab rakendust pigem taustauuringu tegemisel.<sup>68</sup> Seejuures peavad värbajad oluliseks just pildialbumeid, mille pinnalt on võimalik teha järeldusi kandidaadi kohta või saada ka informatsiooni, mida hiljem töövestlusel kasutada.<sup>69</sup>

Silmas pidades sotsiaalmeedia laialdast haaret ka töösuhtes on Euroopa Andmekaitseasutuste Töögrupp on pidanud vajalikuks selles osas seisukohta väljendada. Juunis 2017 avaldas töögrupp värskendatud suunised tööandjatele, milles rõhutatakse, et kandidaadi andmete kogumisel tuleb lähtuda tööandja õigustatud huvist. Pelgalt asjaolu, et isikul on avalik profiil mõnes sotsiaalmeediakeskkonnas, ei ole piisav alus sellelt andmete hankimiseks.<sup>70</sup>

Arvestades andmete töötlemise läbipaistvuse põhimõtet, on töögrupi seisukohad mõistetavad. Teisalt on tööandjal õigustatud huvi oma potentsiaalse tulevase töötaja vastu ning põhiseaduslikult tagatud informatsiooni saamise õigus. K. Visamaa teadustöös on üks intervijueeritavatest välja toonud huvitava mõtte, et temal kui tööandjal polegi sotsiaalmeedias vallatutel peopiltidel figureeriva töötaja vastu midagi, aga pilte võib näha ka mõni konservatiivne klient, kes selle tõttu ettevõttega koostööst loobub.<sup>71</sup> Seega võivad tulevase võimaliku töötaja kohta sotsiaalmeediakontodelt kogutavad andmed ennast siiski õigustada ning kaaluvad seetõttu üle andmesubjekti õigused, eriti silmas pidades seda, et tegemist on nagunii avalikult kättesaadava informatsiooniga.

Senikehtinud IKS-i paragrahv 19 võimaldas kandidaadil nõuda infot enda kohta käivate andmete töötlemise kohta ning vastavalt IKS §-ga 21 oli sedastatud ka õigus nõuda enda

---

<sup>68</sup> K. Visamaa. Veebipõhiste sotsiaalvõrgustike kasutamine töötaja värbamisel. Bakalaureusetöö. Tartu Ülikool. 2011, lk 31 Arvutivõrgus:

[https://dspace.ut.ee/bitstream/handle/10062/28010/visamaa\\_katriin.pdf?sequence=1&isAllowed=y](https://dspace.ut.ee/bitstream/handle/10062/28010/visamaa_katriin.pdf?sequence=1&isAllowed=y) 11.04.2018

<sup>69</sup> sama lk 38

<sup>70</sup> *Article 29 Data Protection Working Party. Opinion 2/2017 on data processing at work.* 08.06.2017, lk 11

<sup>71</sup> Visamaa, lk 38



kohta käivate andmete töötlemise lõpetamist, parandamist, sulgemist ja kustutamist. Need õigused on ka GDPR-i alusel jätkuvalt tagatud, vastavalt artiklitega 15, 16 ja 17, mida täiendavad uue IKS-i §-d 23-27.

Eelmainitud andmete kustutamise nõudmise õigus puudutab muuhulgas ka internetis juba avaldatud andmeid. Näiteks oli kümnekond aastat tagasi tavaks ajakirjanduses avaldada politsei statistikat nädala jooksul rooli tagant tabatud alkoholijoobes või muid õigusrikkumisi toime pannud isikutest, kes tabelites figureerivad kas oma täisnime või leebemal juhul eesnime ja sünniaastaga.<sup>72</sup> Tänapäeval selline tegevus enam lubatud ei ole, kuid vastavaisulisi uudisnupukesi on „*googeldades*“ üsna lihtne leida ning selle alusel isiku kohta negatiivset kuvandit luua, mis omakorda võib mõjutada värbamisotsust.

Õigusele „olla unustatud“ ajendiks oli Euroopa Kohtu 13.05.2014 otsus,<sup>73</sup> mis 1995.a andmekaitse direktiivi tõlgendades andis isikutele õiguse nõuda otsingumootori valdajatelt nende isikuandmeid sisaldavate linkide eemaldamist juhul, kui andmed ei ole enam adekvaatsed, asjakohased või on arvestades andmete kogumise eesmärki ning möödunud aega, ülemääraseid.<sup>74</sup>

Siiski ei saa praktikas õigust olla unustatud üldistada ning loota, et andmed igal juhul kustutatakse, sest „õigusele olla unustatud vastandub avalikkuse õigus mäletada.“<sup>75</sup> Vastavat käsitlust toetab EIKo praktika<sup>76</sup>, mille kohaselt peab ajakirjanduses olema tagatud arhiivide kaitse. Sisuliselt tähendab see seda, et isegi juhul, kui ajakirjanduses on isiku kohta avaldatud ebaõiget infot või ebakohaseid väärtushinnanguid, ei ole nende eemaldamise nõudmine lubatud, kuivõrd see tähendaks ajaloo ümberkirjutamist. EIKo selgitas, et meediaväljaannete internetiarhiivid on kaitstud art 10 mõttes väljendusvabadusena ning arhiividel on oluline roll uudiste jm informatsiooni talletamisel ja vajadusel ka kättesaadavaks tegemisel (nt teadustöö kirjutamisel). Ühiskonna nõ „valvekoera“ funktsiooni kõrval ongi just arhiivide pidamine ja hoidmine teiseks ajakirjanduse oluliseks rolliks.<sup>77</sup>

---

<sup>72</sup> Näiteks 17.09.2004 avaldatud Vooremaa politsei kroonika. Arvutivõrgus: <http://www.vooremaa.ee/politseikroonika-74/> 16.03.2017

<sup>73</sup> Euroopa Kohtu 13.05.2014 otsus nr C-131/12 *Google vs Spain*.

<sup>74</sup> Euroopa Kohtu 13.05.2014 otsus nr C-131/12 *Google vs Spain*. p. 93

<sup>75</sup> V. Peep. Kas alati saab Google'ist välja? - Äripäev 19.11.2015.

<sup>76</sup> EIKo 33846/07 *Wegrzynowski ja Smolczewski vs Poola* 16.07.2013

<sup>77</sup> sama p-d 58-59

Sellest tulenevalt ei ole ka otsingumootoritest alati võimalik nõuda oma andmete eemaldamist, küll on aga väärinfo avaldamise korral mõistlik avaldajalt nõuda paranduse või õiendi tegemist, mis võiks isikukahju mõnevõrra optimeerida.<sup>78</sup>

Magistritöö autori hinnangul vastutab jätkuvalt igaüks oma isikuandmete eest ise ning seetõttu tuleb ennast harjutada jälgima, mida ja kuhu postitatakse, sest läbimõtlematu virtuaalne jalajälg võib tulevikus maksta väärt töökoha.

### 2.2.3. Mitteavalike andmete töötlemine

Kandidaadi kohta andmete hankimiseks on teisigi allikaid, üheks selliseks on soovitajad. Statistikaameti poolt 2014. a avaldatud uuringust selgub, et just tutvuste kaudu töölesaamine on Eesti elanike hulgas kõige populaarsem töölesaamisviis.<sup>79</sup> Andmekaitse Inspeksioon on avaldanud seisukohta, mille kohaselt võiks vastavalt väljakujunenud praktikale eeldada, et märkides soovitaja oma elulookirjeldusse, annab kandidaat sellega nõusoleku soovitajaga ühendut võtmiseks ning oma isikuandmete avaldamiseks.<sup>80</sup> Tööandjal tuleb aga meeles pidada, et soovitajalt on lubatud küsida üksnes selliseid andmeid, mis on vajalikud kandidaadi töölesobivus hindamiseks. Tööandja ei või omaalgatuslikult pöörduda kandidaadi eelmise tööandja poole, et uurida, millise inimesega on tegu ning tema eelmisest kohast lahkumise põhjuseid.

Ülemääraste andmete avaldamise riski on võimalik maandada soovituskirjadega. Kui CV-sse märgitakse üksnes soovitaja nimi ja kontaktandmed, ei oma andmesubjekt tegelikult kontrolli selle üle, millist infot tööpakkujad küsivad ning millist infot soovitaja tema kohta annab, mistõttu võidakse avaldada ülemääraselt või ka ebaõigeid andmeid. Soovituskiri ei välista kõnesid

---

<sup>78</sup> Autori märkus: näiteks on isikut ajakirjanduses põhjendamatult seostatud algatatud kriminaalasjaga. Menetluse käigus see seos kummutatakse, kuid ajakirjanduslik (ning Google'ist kättesaadav) seos on loodud ning selle kustutamise osas puudub isikul nõudeõigus. Küll aga saaks isik nõuda õiendi või paranduse avaldamist, mis seose kõrvaldab. Enim probleeme põhjustab aga asjaolu, et tulenevalt tehnilistest eripäradest salvestub esialgne artikkel Google'i vahemällu ning edaspidi kuvatakse otsingutulemusi, mitte meediaväljaande arhiivist, vaid Google'i enda mälust, seetõttu võib tekkida olukord, kus väljaande arhiivis on olemas parandusega artikkel, kuid Google kuvab jätkuvalt väärinfot sisaldavat artiklit, mille põhjal võivad kolmandad isikud (nt tööandjad) teha valejärelusi.

<sup>79</sup> Eesti Statistikaamet. Muutuv majandus ja tööturg. Tallinn: 2014 lk 97. Arvutivõrgus allalaetav: [http://www.stat.ee/valjaanne-2014\\_muutuv-majandus-ja-tooturg](http://www.stat.ee/valjaanne-2014_muutuv-majandus-ja-tooturg) 15.12.2016

<sup>80</sup> AKI juhend lk 33

eelmisele tööandjale mõistagi täielikult, kuid võimaldab andmesubjektile siiski suuremat kontrolli oma isikuandmete üle, sest soovitajal on alati võimalik soovituskirjale viidata ning lisada, et soovitajal puuduvad rohkema info väljastamiseks volitused.

Andmesubjekti, endise tööandja ja võimaliku tulevase tööandja vahetunde kajastab Tallinna Ringkonnakohtu lahend, milles kohus rõhutab andmesubjekti nõusoleku andmist soovitajale/ eelmisele tööandjale oma isikuandmete avaldamiseks. Nõusolekuna ei saa käsitleda seda, kui elulookirjelduses sisaldub pelgalt viide eelmisele tööandjale. Senikehtinud IKS-i §-le 12 viidates sedastab kohus, et nõusolek, millega lubatakse oma andmeid töödelda, sh kolmandatele isikutele edastada, edastada peab olema väga konkreetne, mh peavad olema määratletud andmete töötlemise eesmärk, andmete koosseis ning ka isikud, kellele on lubatud andmeid edastada. Küll aga mõõnab kohus, et tulevasele tööandjale on lubatud edastada andmeid, mis ei ole isikuandmed, kuid seotud töötaja varasemate tööülesannetega, nt ametiülesannete kirjeldus.<sup>81</sup> Vaatlusalune kaesus on huvitav eelkõige seetõttu, et endise tööandja esindaja näol oli tegemist pahatahtliku isikuga, kelle poolt tulevasele tööandjale edastatud „soovituskirjas“ sisalduvad ebaõiged ja mainet kahjustavad väited töötaja kohta maksid viimasele väärt töökoha, mille kompenseerimiseks tuli õigusvastaselt käitunud tööandjal maksta suhteliselt kopsakas kahjuhüvitis.

Käesoleva töö autor on seisukohal, et lepinguvabaduse põhimõttest lähtuvalt on tööandjatel õigus soovituskirju kandidaatidelt nõuda ning kandideerimisdokumentatsiooni üheks osaks võiks olla spetsiaalne soovitajatele esitatav vorm, milles sisalduksid uue tööandja konkreetsed küsimused eelmisele tööandjale (soovitajale). Sellisel juhul oleks kandidaadil ka alati teada, milliseid andmeid tema kohta küsitakse ning samaaegselt täidaks selline vorm ka GDPR art 7 lg-st 1 tuleneva vastutava töötleja tõendamiskohustuse andmesubjekti nõusoleku olemasolu kohta. Tulevastel tööandjatel tasuks aga eelmainitud kohtulahendi valguses arvestada siiski sellega, et soovitajad saavad jagada üksnes subjektiivsed hinnangud, tööandja võib neid arvesse võtta, kuid need ei tohiks omada määravat kaalu värbamisotsuse tegemisel. Töötaja töölesobivust, isikuomadusi ja oskusi on tööandjal endal võimalik hinnata eelkõige katseperioodi jooksul.

Avalikus teenistuses on ametnike värbamiseks enamasti vajalik avaliku konkursi

---

<sup>81</sup> TlnRnKo 17.01.2017 2-15-9284 p.70

väljakuulutamine,<sup>82</sup> mille korraldamine toimub seaduses ette nähtud alustel. Fikseeritud on nii konkursi väljakuulutamise koht (ametiasutuse ja avaliku teenistuse kesksel veebilehel), kui konkursi kestuse minimaalne aeg.<sup>83</sup> Samuti on reguleeritud ka teave, mida konkursikuulutus peab sisaldama ning kohustus värbamisel ja valikul lähtuma avalikustatud tingimustest ning kandidaatide võrdsest kohtlemisest.<sup>84</sup>

Selle pinnalt võib eeldada, et avalikus sektoris on tõenäosus andmekaitsereeglite või privaatsuse kaitse vastu eksida väiksem, kui erasektoris. Magistritöö autor leiab, et eesmärgiks tohiks seada ülereguleerimise idealiseerimist, kuid samasuguse võrdse kohtlemise ja läbipaistvuse tagamiseks ka erasektoris tuleb tõsta inimeste teadlikkust nii andmekaitse, kui üldise privaatsusõiguse osas.

### 2.3. Kandidaadi isikuandmete säilitamine

Oluline andmekaitseõiguslik aspekt värbamisprotsessis on seotud CV-de jm kandideerimismaterjalide säilitamisega. Töölepinguseaduses konkreetset säilitamist reguleerivat normi värbamismaterjali osas ei sisaldu, mistõttu tuleb lähtuda üldistest isikuandmete säilitamisele kehtestatud nõuetest.

Senikehtivas IKSis on andmete säilitamist sisustatud läbi mitme sätte. IKS § 6 p 2 kohaselt võib isikuandmeid töödelda üksnes määratud ja õiguspäraste eesmärkide saavutamiseks ning andmeid ei või töödelda viisil, mis ei ole nende eesmärkidega kooskõlas. IKS § 24 p 1 kohustab andmetöötajat oma eesmärgi täitnud isikuandmed viivitamata sulgema või kustutama, kui seaduses pole sätestatud teisiti.

GDPR-is on säilitamise piirang ühe põhiprintsiibina välja toodud. Artikli 5 lg 1e kohaselt võib andmeid säilitada üksnes niikaua, kuni need on vajalikud andmete kogumisel seatud eesmärgi täitmiseks. Kui andmed ei ole enam eesmärkide saavutamiseks vajalikud, tuleb need viivitamatult sulgeda või kustutada. Ka uues IKSis on isikuandmete säilitamine eraldi

---

<sup>82</sup> ATS § 16

<sup>83</sup> ATS § 17 lg 1

<sup>84</sup> ATS § 18 lg 1

sättena välja toodud, sedastades, et töödeldavatele andmetele kehtestatakse seaduse või määrusega säilitamise tähtajad. Erandjuhul peab säilitamise tähtaja määrama vastutav töötleja (IKS § 16 lg 1), kelleks antud juhul on tööandja.

Eeltoodust tulenevalt võiks järeldada, et kandideerimisega seotud isikuandmed, tuleks pärast konkursi lõppu viivitamatult kustutada, kuivõrd need on oma eesmärgi täitnud. Siiski on selles osas ette nähtud erand ning kandideerimisega seotud vaidluste tarbeks CV-de säilitamist ei peeta andmete kogumise eesmärgiga vastuolus olevaks.<sup>85</sup> On oluline rõhutada, et kandidaadi andmete säilitamine on üksnes lubatud juhul, kui andmesubjekt ei ole eraldi palunud oma andmete kustutamist ning tööpakkuja on kandidaadilt eelnevalt küsinud nõusolekut andmete säilitamiseks.<sup>86</sup>

Antud küsimuses seisukohta väljendanud Euroopa Nõukogu märgib, et andmed tuleks kustutada kohe, kui on selgunud, et tööpakkumist ei tehta.<sup>87</sup> Värskeemas soovitus on Nõukogu lisanud, et kandideerimisandmed tuleks kustutada ka juhul, kui on selgunud, et kandidaat loobub ise tööpakkumisest.<sup>88</sup>

Siiski on ka Euroopa Nõukogu pidanud õiguspäraseks kandidaadi andmete säilitamist kohtuvaidluste tarbeks, kuid üksnes mõistliku ajavahemiku jooksul.<sup>89</sup> Kuna taaskord on tegemist hinnangulise kriteeriumiga, oleks magistritöö autori hinnangul mõttekam lähtuda üldistest tsiviilvaidlustustähtaegadest.

TsMS § 3 lg 1 annab üldise aluse kohtusse pöördumiseks juhul, kui isik leiab, et tema eeldatavaid ja seadusega kaitstud õigusi või huve on rikutud, erinormidena võimaldavad nii võrdse kohtlemise seaduse (VõrdKS) § 23, kui soolise võrdõiguslikkuse seaduse (SoVS) § 12 diskrimineerimisvaidlusi lahendada nii töövaidluskomisjonis, kui kohtus ning annavad kahjustatud isikule õiguse nõuda ka mittevaralise kahjuna hüvitist kohtu või

---

<sup>85</sup> *Article 29 Data Protection Working Party. Opinion 2/2017 on data processing at work*.08.06.2017, lk 11, allmärkus nr 15

<sup>86</sup> sama

<sup>87</sup> EN soovitus nr R (89) 2 töösuhete eesmärgil kasutatavate isikuandmete kaitse kohta, 1989, p 14.2.

Arvutivõrgus: <https://rm.coe.int/16804b8868> 26.09.2017

<sup>88</sup> *Council of Europe, Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment*, 13.2. 01.04.2015. Arvutivõrgus:

[https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectID=09000016805c3f7a](https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a) 11.04.2018

<sup>89</sup> sama

töövaidluskomisjoni äranägemisel mõistlikus ulatuses. Kahju hüvitamise nõude aegumine mõlema eriseaduse puhul on üks aasta arvates päevast, millal kannatanud isik kahju tekkimisest teada sai või pidi teada saama.<sup>90</sup> Oluline on siinkohal rõhutada, et arvestades lepinguvabaduse põhimõtet, ei ole kahjustatud isikul õigust nõuda töölepingu või teenuste osutamise lepingu sõlmimist või ametisse nimetamist või valimist.<sup>91</sup>

Oma seisukohtade kaitsmiseks peab tööandja olema valmis tõendama, et ei ole diskrimineerimiskeeldu rikkunud, seega, arvestades eelviidatud kaebetähtaega ja kohtumenetluse keskmist asjaamiskiirust, oleks käesoleva töö autori hinnangul mõistlik töökonkursi materjale säilitada ligikaudu poolteist aastat. Kuivõrd ka säilitamine on GDPR art 4 lg 2 tähenduses andmete töötlemine, on ka selleks tegevuseks vajalik andmesubjekti nõusolek, mis on hõlpsasti saavutatav näiteks äraütlevas e-kirjas sisalduva selgesõnalise lausega.

Lisaks diskrimineerimiskeeldu rikkumisele, võib aga (kohtu)vaidlus tõusetuda ka andmete lubamatu töötlemise tõttu, aluse selleks annab GDPRi art 82, mis võimaldab andmesubjektil nõuda temale määruse rikkumise tulemusel tekitatud kahju hüvitamist. Siseriiklik erinorm selleks on VÕS § 1045 lg 1 p 4 või 7.<sup>92</sup> Kui diskrimineerimist keelavad eriseadused nägid ette ka aegumistähtaja, siis GDPRi puhul seda *expressis verbis* kirjas ei ole, mistõttu tuleb magistritöö autori hinnangul lähtuda TsÜS § 150 lg-s 1 välja toodud üldisest kahju õigusvastasest tekitamisest tuleneva nõude aegumistähtajast, mis on kolm aastat ajast, mil isik kahjust ja kahju hüvitama kohustuvast isikust teada sai või pidi teada saama.

Seega sisuliselt peaks tööandja olema igal hetkel valmis oma positsiooni kaitsma. Magistritöö autor leiab, et on ebamõistlik ja liialt koormav kohustada tööandjatel “igaks juhuks” kõikvõimalikke töökonkurssidega seonduvaid materjale määramata aja jooksul talletama. Värbamisprotsessidest tulenevad vaidlused on käesoleval ajahetkel niivõrd harvad, kui mitte olematud nähtused, mistõttu leiab töö autor, et eelpool soovitatud poolteist aastat konkursi lõppemisest alates (st hetkest, kui uue töötajaga sõlmiti tööleping) on tööotsijate andmete

---

<sup>90</sup> VõrdKS § 25 – RT I 26.04.2017, 9 ; SoVS § 14 – RT I 07.07.2015, 11

<sup>91</sup> VõrdKS § 24 lg 4, SoVS § 13 lg 4

<sup>92</sup> Autori märkus: tegemist ei ole iseenesest teineteist välistavate normidega, kuid sõltuvalt asjaoludes tuleb kindlaks teha, kas tegemist on kannatanu isikliku õiguse (sh eraelu puutumatuse) rikkumisega või seadusest tuleneva kohustuse rikkumisega. Ei ole välistatud olukord, kus esinevad mõlemad alused.

säilitamiseks piisav aeg.

Veel üheks säilitamise tähtaja arvestamise mõõdupuuks võiks olla ka katseaja kestus, mis ühtlasi annaks tööandjale võimaluse suhteliselt väheste vahenditega leida asemele uus töötaja juba varem väljaselekteeritud kandidaatide hulgast. Nii TLS § 86 lg 1 kui ATS § 26 lg 2 sätestavad katseaja kestuseks kuni 4 kuud, täiendavalt sedastab ATS § 18 lg 10 paremuselt järgmise kandidaadi ametisse nimetamise alused, sealhulgas ka tähtaja 150 päeva, mille jooksul võib isiku ilma uue konkursi korraldamiseta ametisse nimetada. Seega, jättes eelpool nimetatud vaidlustustähtjad kõrvale, võib sisuliselt ka puht praktilistel kaalutustel pidada õiguspäraseks kandidaadi andmete säilitamist 4 – 6 kuu vältel.

Peatüki vahekokkuvõtteks saab märkida järgmist:

- Kandidaadi andmete töötlemine värbamisel saab toimuda üksnes andmesubjekti nõusoleku alusel (GDPR art 4 lg 2) või vastava juriidilise kohustuse olemasolu korral ka art 6 lg 1c alusel, mispuhul tuleb andmesubjekti töötlemisest teavitada (art 14);
- Kandidaadi andmete kogumisel tuleb tööandjal leida tasakaal töösuhteks vajaliku õigustatud huvi ja andmete minimaalsuse põhimõtte (GDPR art 5 lg 1c) vahel.
- Tööandja on kohustatud kandideerimismaterjali osas kehtestama säilitamise tähtjad (GDPR art 5 ja uus IKS § 16).

### 3. ÕIGUSTE TASAKAALUSTAMINE TÖÖLEPINGU AJAL

Võrreldes teiste võlaõiguslike lepingutega, on töölepingulises suhtes tööandjal kontrollipositsioon (TLS § 1 lg 1). Vastav õigus on tööandjale tagatud põhiseadusliku ettevõtlusvabaduse raames (PS § 31), millega on isikutele antud õigus tegeleda majandustegevusega ning teenida sellest tulu.<sup>93</sup> Sellise tegevusega peab aga paratamatult kaasas käima ka õigus oma ettevõtet juhtida ning vabalt otsuseid vastu võtta.<sup>94</sup> Arvestades, et majandustegevuse eesmärk on tulu saamine, on tööandja peamisteks huvideks kvalifitseeritud töötajate leidmine ja hoidmine, aga ka oma ärisaladuse kaitsmine ning konkurentsi piiramine, mis omakorda eeldab töötajate kohta mitmesuguse informatsiooni kogumist.<sup>95</sup>

Vastukaaluks tuleb aga töötajatele tagada nende eraelu ja isikuandmete kaitse. Üldjoontes peaks töösuhetes kehtima reegel, et sekkumine töötaja privaatsusesse on tööandjale küll lubatud, kuid seda tuleb teha viisil, mis on üksnes „hädavajalik töösuhte mõistlikuks ja tõrgeteta toimimiseks.“<sup>96</sup> Arvestades aga teisenenud töökeskkonda on tasakaalupunkti leidmine üha raskem.

#### 3.1. Töötaja isikuandmete kogumine

Senikehtiva IKS-i kohaselt on üldjuhul on töötaja puhul lubatud koguda ja säilitada üksnes selliseid andmeid, mis on vajalikud töölepingust tulenevate tööülesannete või seadusest tulenevate kohustuste täitmiseks (nt maksukohustused) ehk andmed, mille vastu on tööandjal õigustatud huvi<sup>97</sup>

GDPR art 6 alusel võiksid töösuhte puhul seaduslike alustena kõne alla tulla andmesubjekti nõusolek (lg 1a); lepingu täitmise vajadus (lg 1b); tööandja juriidiline kohustus, nt maksuõiguslik (lg 1c) ning tööandja õigustatud huvi (lg 1f). TLS-is on andmete kogumise põhimõtte sätestatud paragrahvis 11, samuti viidatakse osaliselt töölepingu sõlmimiseks

<sup>93</sup> RKPKo 06.03.2002, 3-4-1-1-02; 06.07.2012, 3-4-1-3-12, p 41

<sup>94</sup> Erlich, Henberg, Kask. Põhiseaduse kommentaarid §-le 31, p 5

<sup>95</sup> Henberg (vnr 1), lk 560

<sup>96</sup> AKI juhendmaterjal, lk 9.

<sup>97</sup> IKS § 14 lg 1 p 4 ja TLS § 15 lg 2 p 8.



vajalikele andmetele paragrahvis 5. Töölepinguseaduse seletuskiri soovib töötajate andmete kogumisel lähtuda mõistlikkuse põhimõttest ning arvestada tegevus- või kutseala tavasid ja üldist praktikat.<sup>98</sup>

Soome privaatsusõigust töösuhetes reguleeriv seadus märgib ühemõtteliselt, et tööandjal lubatud on üksnes selliste andmete kogumine, mis on otseselt vajalikud töösuhte toimimiseks. Lisaks on sätestatud, et ka töötaja nõusolekul kogutud mistahes muud vajalikkuse kriteeriumist kõrvalekalduvad kokkulepped töötaja isikuandmete töötlemise osas on keelatud.<sup>99</sup>

Avalikus teenistuses on olukord mõnevõrra keerulisem, kuna asutusel on kohustus oma töötajate üle arvestust pidada. Riigi personali- ja palgaarvestuse andmekogu definitsiooni ning üldised põhimõtted sätestab ATS § 106. Täpsustav kasutusala ning andmekogusse esitatavad andmed on kehtestatud Vabariigi Valitsuse määrusega,<sup>100</sup> mis sätestab kinnise loeteluna nimekirja kogusse kantavatest töötaja andmetest (sh täisnimi, sünniaeg või isikukood, sugu, haridustase, keeleoskus jms).

Ajas muutuvate dokumentide (nt. tervistõendid ja karistusandmed) säilitamine ei ole iseenesest töösuhte jaoks enam vajalik, kuid Andmekaitse Inspektsiooni soovitude kohaselt võiks neidki värbamisotsuste vaidlustamise tähtaja saabumiseni säilitada. Haridust ja kvalifikatsiooni tõendavate dokumentide (sh koopiate) hoidmine on vajalik üksnes siis, kui tööandjal tuleb neid asjaolusid tõendada kolmandatele isikutele.<sup>101</sup> Näiteks juristide puhul, kes esindavad kohtumenetluses menetlusosalisi on TsMS § 218 lg 1 p 2 kohaselt nõutav magistrakraad või sellele vastav kvalifikatsioon. Kui advokaadi puhul tulenevalt Advokatuuriseaduse<sup>102</sup> § 23 lg-s 1 sätestatud kutsenõuetest tulenevalt magistrakraadi olemasolu eeldatakse, tuleb juristil oma haridust igakordselt diplomiga tõendada.

Seaduse alusel kogutavate andmete hulka võivad tööülesannete olemusest ja töökoha reeglitest kuuluda ka näiteks andmed töötaja rõivasuuruse või jala numbri kohta (nt. juhul, kui

---

<sup>98</sup> TLS seletuskiri lk 24

<sup>99</sup> *Laki yksityisyyden suojasta työelämässä* § 2 lg 3

<sup>100</sup> Vabariigi Valitsuse 16.05.2013 määruse nr 23 Riigi personali- ja palgaarvestuse andmekogusse andmete esitamise ja arvestuse toimingute teostamise kord § 6. RT I, 07.04.2016, 7

<sup>101</sup> AKI juhendmaterjal lk 36

<sup>102</sup> Advokatuuriseadus – RT I 20.04.2017, 4

töökohal on kehtestatud vormiriietuse vms kandmise nõue). Andmeid laste kohta on tööandjal vaja puhkuste ja mõnes ettevõttes ka perele mõeldud soodustuste või ürituste jaoks, viimasel juhul on Andmekaitse Inspektsiooni hinnangul siiski töötajal võimalik andmete avaldamisest keelduda<sup>103</sup> või anda neid välja töötajale endale sobivas mahus.

Teatud ametnike puhul on andmete avaldamise osas seadusandja ette näinud lisakohustuse, nimelt sätestab Korruptsioonivastase seaduse<sup>104</sup> (KVS) § 3 lg 2 p 2, et ametnik peab seaduses sätestatud juhul ja korras avaldama oma huvid vastavas deklaratsioonis. Tulenevalt KVS § 12 lg-st 1 on deklaratsioonide eesmärgiks teadvustada deklarandi ametikohustuste täitmist mõjutada võivad huvid ning muuta need kontrollitavaks. Vastavalt KVS § 14 lg-le 1 on deklareeritavateks huvideks eelkõige andmed kinnisomandi ja sellele seatud asjaõiguste kohta, registreeritud sõidukid, väärtpaberid ja varalised kohustused.

Eraõiguslikus töösuhtes puudub töötajal üldjuhul kohustus sellist tüüpi varanduslikke andmeid avaldada (v.a krediidi- ja investeerimisasutuste töötajad, kelle jaoks tuleneb vastav kohustus seadusest<sup>105</sup>). Küll aga võiks magistritöö autori hinnangul kõne alla tulla tööandja õigus nõuda töötajalt andmeid temale kuuluvate osaluste kohta ettevõtetes TLS § 15 lg 1 p 8 alusel olukordades, kus tööandja põhitegevusalal toimub äärmiselt tugev konkurents (näiteks ravimifirmad) ning töötaja osalus teistes ettevõtetes võiks tööandja positsiooni turul ja/või mainet seeläbi negatiivselt mõjutada. Sellisel juhul oleks tööandjal andmete väljanõudmiseks õigustatud huvi.

Andmete kogumisel ja ka hilisemal säilitamisel on oluline eristada mõisteid “andmed” ja “dokument.” Dokument võib sisaldada andmeid (nt tööleping), kuid andmeteks võib pidada ka suuliselt edastatud infot. Praktikas võrdsustatakse andmed sageli dokumendiga ja üldjuhul nõutaksegi kõiki andmeid üksnes dokumendi kujul.<sup>106</sup> Andmekaitse Inspektsioon soovib igakordselt kaaluda, kas originaaldokumendi säilitamine on vajalik või piisab sellelt üksnes oluliste andmete väljakirjutamisest, kuivõrd originaaldokumendid sisaldavad sageli ka andmeid kolmandate isikute kohta, mis andmetöötluse eesmärke silmas pidades ei pruugi olla asjakohased, näitena on AKI välja toonud, et kui töötaja esitab lapse vanuse tõendamiseks

---

<sup>103</sup> AKI juhendmaterjal lk 36

<sup>104</sup> Korruptsioonivastane seadus – RT I 17.11.2017, 29

<sup>105</sup> Nt. Krediidiasutuste seadus § 49

<sup>106</sup> AKI juhendmaterjal lk 77

sünnidokumendi, piisab üksnes sellelt andmete väljakirjutamisest ning dokumendi eraldi säilitamist ei ole vaja. AKI hoiatab, et mida rohkem andmeid kogutakse, seda rohkem on andmeid, mida kaitsta ja seda suurem on kahju, mis tekib siis, kui andmetele pääseb ligi selleks õigustamata isik.<sup>107</sup>

Seega tuleb töötaja isikuandmete kogumisel lähtuda tööandja õigustatud huvist, kogudes siiski üksnes sellist informatsiooni, mis on töösuhte tõrgeteta toimimiseks mõistlikult vajalik.

### 3.2. Töötaja isikuandmete avaldamine

Nagu varasemalt selgitatud saab töösuhtes töötaja andmete töötlemine sh ka avaldamine toimuda kas töötaja nõusoleku alusel, temaga sõlmitud töölepingu täitmiseks või tööandja õigustatud huvi korral, eeldusel, et see kaalub üles andmesubjekti huvid või põhiõigused ja – vabadused.<sup>108</sup>

Tänapäeval on saanud tavaks, et ettevõtte/ asutusel on kodulehekül, millel tutvustatakse organisatsiooni olemust, väärtuseid, tegevusi ja ka isikkoosseisu. Viimase osas leidub praktikas väga erinevaid näiteid – mõnel juhul piirduakse kodulehel üksnes töötaja nimele viitamisega, teisel juhul on juurde lisatud pilt, kontaktandmed ja suhteliselt detailne elulugu. Eriti leiab selliseid võrdlemisi personaalseid isikutuvustusi just eraettevõtete kodulehtedelt<sup>109</sup>. Avaliku sektori asutuse lehtedel leiab teinekord hoopis kitsenduse sellele, et lehel avaldatud andmeid on lubatud kasutada üksnes ametialaseks suhtluseks.<sup>110</sup>

Töölepinguseaduses vastavat olukorda reguleerivat sätet ei ole. Samuti puudub tegelikult üldse igasugune kohustus veebilehe vms olemasoluks ning ettevõtte võibki üksnes eksisteerida Äriregistris ning olla kättesaadav seal kajastatud rekvisiitidel. Siiski on ettevõtted üha tihenevas konkurentsisis pigem hakanud kodulehe kõrvale ka sotsiaalmeediaprofiile looma.

---

<sup>107</sup> AKI juhendmaterjal, lk 77

<sup>108</sup> GDPR art 6 lg 1a, 1b ja 1f

<sup>109</sup> Näiteks Telia Eesti AS. Arvutivõrgus: <https://www.telia.ee/ettevottest/saame-tuttavaks> 05.03.2018

<sup>110</sup> Näiteks Justiitsministeeriumi koduleht. Kättesaadav: <http://www.just.ee/et/kontakt> 04.04.2017

Avalikus teenistuses on asutusesisese veebilehe pidamise kohustus Riigikogu Kantsleil, Vabariigi Presidendi Kantsleil, Õiguskantsleri Kantsleil, Riigikontrollil, kohtutel, valitsusasutustel ja avalik-õiguslikel juriidilistel isikutel,<sup>111</sup> viidatud asutuste puhul on reguleeritud ka veebilehe pidamise ja sellel avaldamise nõuded.<sup>112</sup>

Vastavalt avaliku teabe seadusele tuleb muuhulgas avalikustada ametnike ametijuhendid,<sup>113</sup> ametiasutuste koosseisud ja neis asutustes ettenähtud ametikohti täitvate ametnike ees- ja perekonnanimed, hariduse ja eriala, telefoninumbrid ning elektronpostiaadressid<sup>114</sup> ja ametnike palga ja teenistusülesannete täitmisega seonduvad andmed.<sup>115</sup>

Magistritöö autor ei näe probleemi selles, kui ettevõtte/ asutuse kodulehel avaldatakse töötaja nimi koos näiteks üldtelefoniga, kui tegemist on sellise töötajaga, kelle töö olemusest on nõutav, et ta oleks klientidele või koostööpartneritele töö ajal kättesaadav. Arusaadavalt on sellisel juhul tegemist olukorraga, kus isikuandmete avalikustamine on töötajaga sõlmitud lepingu täitmiseks või tuleneb vastav avaldamise kohustus seadusest (ametnike palgad ja ametijuhendid).

Töötaja kirjaliku nõusoleku küsimine peaks aga töö autori hinnangul olema nõutav olukordades, kus avaldatakse lisaks eeltoodule ka e-posti aadress ning mingis vormis elulugu. Selline kinnitus võiks näiteks sisalduda juba töölepingus või selle lisas. Siiski tuleb arvestada, et nii fotode kui elulugude avaldamise puhul on tegemist mõningase riivega töötaja privaatsfääri, mistõttu tuleks nende andmete vajalikkust töösuhte seisukohalt vaadatuna igakordselt hinnata. On tõepoolest ametikohti, kus töötaja varasem elu- ja töökäik võib mõjutada kliendisuhteid ning tagada tööandjale parema maine. Näiteks võivad kliente „meelitada“ õppeasutused, milles töötaja on omandanud hariduse või täiendõppe, samuti võib teatud juhtumitel määrava tähtsusega olla töötaja varasemad töökohad või portfoolio. Ka võib kliendisuhetele teinekord kasuks tulla seegi, et töötaja harrastab purjetamist või lohesurfi ning on vanemaks kolmele lapsele. Küll aga tuleb silmas pidada, et tööandjal ei ole õigust töötajalt selliste andmete avaldamist nõuda ega ilma töötajata nõusolekuta ka eelviidatud eraelulisi

---

<sup>111</sup> AvtS § 31 lg 1

<sup>112</sup> AvtS § 32

<sup>113</sup> AvtS § 28 lg 1 p 5

<sup>114</sup> AvtS § 28 lg 1 p 6

<sup>115</sup> AvtS § 28 lg 1 p 25

andmeid omavoliliselt ettevõtte/ asutuse kodulehel avaldada.

### 3.3. Kommunikatsiooni jälgimine ja sõnumisaladuse kaitse

Tänapäeval on levinuim suhtlemise viis Interneti vahendusel toimuv elektrooniline kommunikatsioon (e-kiri, Skype'i suhtluskeskkond, Facebook Messenger, Snapchat vms). Enamasti luuakse töötajale tööandja domeeninimega e-posti aadress, mida töötaja kasutab tööalaseks suhtluseks ning tööülesannete täitmiseks. Olenevalt ettevõtte spetsiifikast võib e-postile lisanduda veel mõni alternatiivne suhtluskeskkond.

Andmekaitse Inspektsiooni juhendmaterjalis märgitakse, et tõenäoliselt ei ole töötajatel endal aimugi, millist informatsiooni nende postkastist kätte võib saada<sup>116</sup> ning millise tervikpildi nende andmete põhjal luua võib. Oluline on välja tuua, et puudutatud ei ole mitte üksnes töötaja, vaid põhimõtteliselt ka kõik need isikud, kellega või kelle teemadel suheldud on. Näiteks võib vestlusest õpetajaga saada infot töötaja lapse tervise seisundi või õpitulemuste kohta. Võibolla on töötaja suhelnud krediidasutusega kodulaenu või autoliisingu teemadel või lahanud sõbrannaga kellegi kolmanda tuttava perekondlikke probleeme.

Isikutevahelisele kommunikatsioonile on küll tagatud põhiseaduslik kaitseõigus, kuid Eesti tööõiguse kontekstis on tegemist reguleerimata valdkonnaga. Soomes seevastu on kõnealune valdkond eriseadusega reguleeritud, milles võrdlemisi detailselt sedastatakse nii töötaja e-kirjade avamine, kui nende taastamine tööandja poolt.<sup>117</sup> Seejuures kohustub tööandja mõlemal juhul koostama aruande, milles muuhulgas kajastub, miks e-kiri avati, kelle poolt ja millistel eesmärkidel ning edastama aruande viivitamata puudutatud töötajale.<sup>118</sup>

Ka Ühendkuningriigi andmekaitseasutuse juhendis rõhutatakse, et kui tööandja soovib töötajate elektroonilist kommunikatsiooni mingil viisil jälgida, tuleb esmalt sisse seada vastav kord ning seda töötajatele arusaadavalt tutvustada.<sup>119</sup> Samuti selgitatakse, et eelviidatud korras peaks sisalduma ka kommunikatsioonivahendite isiklikuks otstarbeks kasutamise

---

<sup>116</sup> AKI juhendmaterjal lk 60

<sup>117</sup> *Laki yksityisyyden suojasta työelämässä* § 6 lg-d 19 ja 20

<sup>118</sup> sama

<sup>119</sup> *Information Commissioner's Office. The Employment Practices Code*, lk 68

juhised.<sup>120</sup>

Kui TLS sedastab lakooniliselt tööandja kohustusena üksnes töötaja põhiõiguste austamise, siis tulenevalt GDPRi art-st 32 lasub tööandjal, kui vastutaval töötajal kohustus kasutusele võtta organisatsioonilised, füüsilised ja infotehnilised turvameetmed isikuandmete kaitseks ning turvalisuse tagamiseks. Andmekaitse Inspektsiooni hinnangul võib sellisteks meetmeteks lugeda muuhulgas kasutajatunnuseid ja parooli arvutivõrku sisenemiseks ning ekraanilukustamist töökohalt lahkumise ajaks.<sup>121</sup>

Kuna mõningane sekkumine töötaja privaatsusesse, sh kommunikatsiooni, on töösuhetes paratamatu, lähtutakse sekkumises hädavajalikkuse kriteeriumist - tööandjal on lubatud sekkuda töötaja privaatsusesse üksnes niivõrd, kui see on hädavajalik töötamise mõistlikuks korraldamiseks. Hädavajalikkus on eelkõige hinnangute küsimus ning siinkohal peaksid tööandja ja töötaja leidma oma huvide ja õiguste ristumise keskpunkti.

Ühelt poolt on töötajal õigus eraelule, isikuandmete ja sõnumisaladuse kaitsele, teisalt, kui töötaja allub tööandja kontrollile, siis on tööandjal ka õigus kontrollida ka reaalset töö tegemist,<sup>122</sup> sealhulgas ka töötajale tööandja poolt usaldatud elektrooniliste töövahendite sihipärast kasutamist, mis omakorda hõlmab sisuliselt ka õigust lugeda töötaja e-kirju.<sup>123</sup>

Mõnevõrra ebaõnnestunult sedastas EIKo 2016. aasta alguses tööandja õiguse töötaja erakirju lugeda lahendis *Barbulescu vs Rumeenia*,<sup>124</sup> misjärel kriitikud üle Euroopa kirjutasid oma blogides, et „EIKo on andnud nuhkimisele roheline tule“<sup>125</sup> ja „privaatsus töökohal on nüüd „surnud.““<sup>126</sup>

---

<sup>120</sup> *Information Commissioner's Office. The Employment Practices Code*, lk 68

<sup>121</sup> AKI juhendmaterjal lk 61

<sup>122</sup> Vastava õiguse sedastab ka TLS § 28 lg 1 p 11, rõhutades, et kontrollimine peab toimuma viisil, mis ei riku töötaja põhiõiguseid.

<sup>123</sup> Autori märkus: silmas on peetud töötaja tööalasele postiaadressile laekunud tööga seotud e-kirju. Töötaja erakirjade lugemine vm tegevus on lubamatu isegi juhul, kui need on saabunud tööaadressile.

<sup>124</sup> EIKo 61496/08 *Barbulescu vs Rumeenia* 12.01.2016.

<sup>125</sup> J.Smart. *Green light for "Big brother" lurking?* - Bevan Brittan õigusblogi. 28.01.2016. Arvutivõrgus: <https://www.bevanbrittan.com/insights/articles/2016/ee-green-light-for-big-brother-lurking-investigations-at-work/> 14.11.2016

<sup>126</sup> S. Peers. *Is Workplace Privacy Dead? Comments on the Barbulescu judgment.* - EU Law Analysis õigusblogi. 14.01.2016. Arvutivõrgus: <http://eulawanalysis.blogspot.com/2016/01/is-workplace-privacy-dead-comments-on.html> 14.11.2016

Otsus tundus esmapilgul olevat täielikult vastuolus EIKo varasema praktikaga, näiteks oli lahendis *Halford vs Ühendkuningriigid* sedastatud, et isikul on ka töökohas “mõistlik ootus privaatsusele”<sup>127</sup> ning lahendis *Copland vs Ühendkuningriigid* leitud, et kommunikatsiooni jälgimine töökohal riivab isiku privaatsust.<sup>128</sup> Oluline erinevus peitus aga selles, et kui mainitud juhtudel oli jälgimine toimunud olukorras, kus töötajal eksisteeris tema enda arusaamist mööda mõistlik ootus privaatsusele, siis *Barbulescu* töökohal oli kehtestatud ranged töösisekorra eeskirjad, mis keelasid tööandja poolt antud elektrooniliste töövahendite ja seadmete (sh klientide nõustamiseks mõeldnud *Yahoo Messenger* keskkonna) isiklikel eesmärkidel kasutamise, kuid *Barbulescu* otsustas keeldu eirata. Kui tema tööandjal tekkisid tema suhtes kahtlused tööülesannete mittetäitmise osas, otsustas tööandja läbi viia pistelise kontrolli, mille käigus ilmnisid muuhulgas ka *Barbulescu* isiklikud internetivestlused, mis viisid töölepingu lõpetamiseni. EIKo on otsuse punktis 57 nõustunud siseriiklike kohtutega selles, et kuivõrd *Barbulescu* ülesanded hõlmasid ka klientide nõustamist läbi *Yahoo Messengeri* ja ettevõttes oli keelatud *Messenger*’i kasutamine isiklikel eesmärkidel, oli tööandjal vestlusi kontrollides õigustatud ootus, et leiab eest üksnes töömaterjale, ning seetõttu oli riive *Barbulescu* eraellu õiguspärane.

Sügisel 2017. tegi aga EIKo suurkogu asjas vastupidise otsuse põhjusel, et töötajat oli küll informeeritud sellest, et ettevõtte IKT-vahendeid ei tohi kasutada isiklikel eesmärkidel, kuid tuvastamata jäi, kas töötajat oli eelnevalt teavitatud ka kommunikatsiooni võimalikust jälgimisest ja selle ulatusest.<sup>129</sup>

EIKo märgib lahendis, et arvestades IKT valdkonna kiiret arengut ning sellest tulenevalt ka erinevate jälgimisvõimaluste kasvu, tuleb jätkuvalt kindlustada õiguslik proportsionaalsus ja ka menetluslikud tagatised omavoli vastu. Seda silmas pidades andis EIKo riiklikele kohtutele suunised, mida ka tööandjad jälgimismehhanismide kasutuselevõtmisel võiksid silmas pidada:

- kas töötajaid on teavitatud võimalikust jälgimisest, selle ulatusest ning mõjust töötajale;

---

<sup>127</sup> EIKo 20605/92 *Halford vs Ühendkuningriik*. 25.07.1997.

<sup>128</sup> EIKo 62617/00 *Copland vs Ühendkuningriik*. 03.04.2007.

<sup>129</sup> EIKo 61496/08 *Barbulescu vs Rumeenia*. 05.09.2017 p. 133

- kas eksisteerib õigustatud huvi jälgimiseks ning jälgimise eesmärk
- kas jälgimiseks on valitud meetod, mille mõju on töötaja privaatsusele väikseim;
- kas töötajatele on tagatud kaitsemeetmeid (näiteks teavitust kontrollist või jälgimisest).<sup>130</sup>

Andmekaitse Inspeksioon on seisukohal, et isegi kehtestades töökohal nulltolerants töölase e-posti aadressi kasutamiseks isiklikel eesmärkidel, ei ole võimalik garanteerida, et sellele ei saabu ega sattu ühtegi erakirja (näiteks on eesnimi perenimi kombinatsioon internetist otsingumootoritega väga lihtsalt leitav ning seetõttu võib tööpostkasti sattuda isiklik kiri kolmandalt isikult ilma, et töötaja ise sellele kuidagi kaasa aitaks).<sup>131</sup> Teisalt ei saa ka kuidagi välistada tööandja õigust pääseda töötaja postkasti, kuivõrd faktiliselt on tegemist tööandja omandiga ning tahes-tahtmata võib tekkida ootamatuid olukordi, kui ettevõtte tõrgeteta toimimiseks on eemaloleva töötaja kommunikatsioonivahenditesse pääsemine hädavajalik.

Internetikasutuse laialdast levikut ning erinevaid suhtlemise võimalusi silmas pidades tasub peatuda ka töökeskkonnavälistel suhtluskanalitel (nt blogid, Facebooki avalikud grupid, Twitter jms), mille üle tööandjal puudub igasugune kontroll, kuid mis ometigi võivad tema (majanduslikke) huve kahjustada. Greete Kempel on oma magistritöös välja toonud märkimisväärse koguse juhtumeid, kus sotsiaalmeedia kasutusest on töösuhtes põhjustatud tööandjale mainekahju. Näiteks 2007 aset leidnud juhtum, kus SEB panga tellerid toonase ülipopulaarse suhtluskeskkonna Orkut vahendusel mõnitasid panga kliente, teadmata, et nende vestlus on avalik; 2012 toimus samalaadne intsident kohvik Komeedi töötajatega, kus ettekandjatel jagus krõbedaid väljendeid nii klientide kui kohviku enda aadressil; 2013 naeruvääristasid ühe Tallinna mahlabaari müüjad ettevõtte kliente Facebookis.<sup>132</sup>

Sotsiaalmeedia väärkasutusest leiab sarnaseid juhtumeid ka avalikust sektorist. Näiteks 2012 riputas haiglaõde raskelt haige väikelapse pildi Facebooki, lisades juurde kommentaari “panin esimest korda 2-kilosele lapsele kanüüli...jeei”; samast aastast pärineb ka ühe kaitseväelase Facebooki postitus, milles ta teravalt kritiseeris Afganistaanis hukkunud

<sup>130</sup> EIKo *Barbulescu vs Rumeenia*. 2017 p 121

<sup>131</sup> AKI juhendmaterjal lk 61

<sup>132</sup> G. Kempel. Sotsiaalmeedia töösuhetes: tööandjate hinnangud ja kogemused. Magistritöö. Tartu Ülikool 2014, lk 26-27 Arvutivõrgus: [http://dSPACE.ut.ee/bitstream/handle/10062/42383/kempel\\_greete\\_ma\\_dsp.pdf?sequence=3](http://dSPACE.ut.ee/bitstream/handle/10062/42383/kempel_greete_ma_dsp.pdf?sequence=3) 19.04.2018



kaaskaitsevälend; 2014 esitas toonane rahandusminister Jürgen Ligi lahkumisavalduse, olles varem Facebookis toonast haldusministrit Jevgeni Ossinovit nimetanud “sisserändaja pojaks roosast erakonnast.”<sup>133</sup>

G. Kempeli poolt magistritöö raames läbiviidud uuringust selgus ühemõtteliselt, et tööandjad eeldavad, et töötaja on oma töökohaga seotud ka väljapool tööaega.<sup>134</sup> See aga tähendab seda, et töötajad peaksid ka tööst vabal ajal kandma ettevõtte väärtuseid ja hoidma ärisaladust ning mitte avalikes kanalites oma tööandjat või kliente kiruma. Puht objektiivsetel põhjustel puudub aga tööandjal selles osas igasugune kontroll ja negatiivsed intsidendid saavad avalikuks üksnes juhuste tõttu (nt ajakirjanduse vahendusel või läbi tuttava). Eeltoodust tulenevalt on tööandjatel üha keerulisem kontrolliõigust teostada ning tagada oma huvide realiseerimine.

Sotsiaalmeedia ebapädevast kasutusest tingitud mainekahju vältimiseks oleks ettevõttes mõistlik välja töötada käitumisjuhised, mille alusel töötajaid sotsiaalmeedia osas koolitada võiks.<sup>135</sup> Ka käesoleva magistritöö autor on seisukohal, et kuigi tööandjal sisuliselt puudub kontroll erakanalites toimuva suhtluse osas, võiks ettevõtte sisekorras olla välja toodud ka sotsiaalmeedia kasutamine sh töövälisel ajal. Võttes aga arvesse EIKo hiljutisi suuniseid,<sup>136</sup> peaks aga töötajale olema kaitsemeetmena tagatud see, et juhul, kui tema kommunikatsiooni on mistahes põhjusel tööandja poolt vaadatud, peaks sellele järgnema ka vastav teavitamine, mis tuleks kirjalikus vormis fikseerida, et vältida hilisemaid arusaamatusi ja õigusvaidlusi.

### 3.4. Metaandmed ja privaatsus

Kuivõrd valdav osa tööst tehakse nii era- kui avalikus sektoris ära elektrooniliselt, tekitab see asjaolu hulgaliselt andmeid ka dokumentide loomise kohta, milliseid on võimalik seostada ka konkreetsete isikutega. Lihtsustatult kujul on metaandmed teave, mis tekib infotehnoloogiliste

---

<sup>133</sup> H. Urbel. Tööle kandideerijate internetipõhine taustauuring ja töötajate monitoorimine: meediatettevõtte näitel. Magistritöö. Tartu Ülikool 2015, lk 21-22 Arvutivõrgus:  
[http://dspace.ut.ee/bitstream/handle/10062/46890/urbel\\_henrik\\_ma\\_2015.pdf](http://dspace.ut.ee/bitstream/handle/10062/46890/urbel_henrik_ma_2015.pdf) 19.04.2018

<sup>134</sup> Kempel, lk 43

<sup>135</sup> sama, lk 93

<sup>136</sup> *Barbulescu vs Romania* (viide nr 126)

vahendite kasutamisel ning annab teada, kes, mida, kus ja millal tegi.<sup>137</sup> Sisuliselt on tegemist nõ virtuaalsete jalajälgedega, mille abil on muuhulgas võimalik arvutikasutajaid tuvastada.

Metaandmete õigusliku määratluse kohaselt on tegemist andmetega, mis kirjeldavad dokumentide konteksti, sisu ja struktuuri ning nende haldamise ajalugu<sup>138</sup> ning tagavad dokumentide autentsuse, usaldusväärsuse, kasutatavuse ja terviklikkuse läbi aja ning võimaldavad nende mõistmist.<sup>139</sup>

Metaandmete töötlemine on vajalik eelkõige infoturbe kontekstis, kuivõrd nende abil on võimalik tuvastada ründeid andmesidevõrgu ja selle kasutajate vastu, kuid samaaegselt võimaldavad metaandmed ka arvutikasutajate (ehk konkreetsete isikute) tuvastamist. Isikuandmetena käsitleb metaandmeid ka GDPR art 4 lg 1, lisades isikuandmete mõiste loetellu *expressis verbis* ka võrguidentifikaatorid.

Metaandmeid võib pidada isegi olulisemaks kui dokumendi tegelikku sisu.<sup>140</sup> Näiteks on üksnes metaandmete põhjal võimalik kokku panna suhteliselt põhjalik isiku profiil sealhulgas teada saada millal ta magab, tema religioosne kuuluvus, sotsiaalne positsioon ja staatus.<sup>141</sup> Sarnast metoodikat kasutavad muuhulgas ka USA julgeolekuorganid võimalike terroristide ja kuritegelike ühenduste kaardistamiseks.<sup>142</sup>

Metaandmete olulisust rõhutatakse ka Kanada Andmekaitseasutus oma raportis, milles uuritakse IP-aadressi mõju isikute privaatsusele ning leitud, et üksnes IP-aadressi alusel on ilma erilise pingutuseta võimalik kokku panna isiku tervikprofiil tema igapäevastest tegevustest ja harjumustest.<sup>143</sup>

---

<sup>137</sup> AKI juhendmaterjal. Metaandmed ja privaatsus. 2015 lk 4. Arvutivõrgus:

[http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/Juhised/Metaandmed.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/Metaandmed.pdf) 16.02.2017

<sup>138</sup> Vabariigi Valitsuse 26.02.2001 määrus nr. 80 „Asjaajamiskorra ühtsed alused“ § 6 lg 1<sup>1</sup> p. 2. RT I, 26.08.2015, 6

<sup>139</sup> Informatsioon ja dokumentatsioon. Dokumendihaldusprotsessid. Dokumentide metaandmed. EVS-ISO 23081-1

<sup>140</sup> AKI juhendmaterjal. Metaandmed ja privaatsus, lk 8

<sup>141</sup> E. Nakashima. *Metadata reveals the secrets of social position, company hierarchy, terrorist cells. The Washington Post*, June 15, 2013

<sup>142</sup> sama

<sup>143</sup> *The Office of the Privacy Commissioner. What an IP Address Can Reveal About You. A report prepared by the Technology Analysis Branch of the Office Privacy Commissioner of Canada. Quebec: May 2013, lk 3.*

Kättesaadav: [https://www.priv.gc.ca/media/1767/ip\\_201305\\_e.pdf](https://www.priv.gc.ca/media/1767/ip_201305_e.pdf) 03.04.2017

Metaandmete puhul ongi üheks kõige iseloomulikumaks ja ehk ka arusaadavamaks näiteks IP-aadressid,<sup>144</sup> mille ülesanne on võimaldada andmete edastamist võrkude vahel, ehk sisuliselt näidata kuhu mingid andmed tuleb saata.<sup>145</sup> Tehnoloogias liigitatakse IP-aadressid staatilisteks ehk püsivateks ning dünaamilisteks ehk ajutisteks, mis määratakse igaks internetiühenduseks eraldi, iga uue ühenduse korral vana aadress kustutatakse ja asendatakse uue IP-ga. See on oluline just privaatsuse kontekstis, sest arvutikasutajat on seetõttu raskem tuvastada.<sup>146</sup>

Vaatamata sellele on Euroopa Kohus sedastanud, et ka dünaamilised IP-aadressid võivad teatud juhul olla käsitletavad isikuandmetena, kuigi need ei kujuta endast teavet, mis seostuks otseselt konkreetse isikuga. Siiski võib olla isiku tuvastamine võimalik kolmandast isikust sideteenusepakkuja kaudu,<sup>147</sup> seda siiski tingimusel, et tuvastamine toimuks seaduslikel alustel ning seda kontrolliks kohus.<sup>148</sup>

Seega tuleb igal juhul jaatada metaandmete olulisust. Siiski tõstatab see omakorda küsimuse, millises mahus ning millise aja jooksul on õiguspärane metaandmeid sisaldavate dokumentide säilitamine just käesoleva magistritöö teemat silmas pidades, eeldades, et suurem osa tööd tehakse ära elektrooniliselt ning päevas luuakse sadu dokumente, mis eeltoodut arvesse võttes kõik sisaldavad vähemal või rohkemal määral isikuandmeid.

Magistritöö autori hinnangul tuleb siinkohalgi lähtuda mõistlikkuse põhimõttest. Esiteks on töölepingutega võimalik fikseerida asjaolu, et kõik töösuhte jooksul loodavad dokumendid (sh elektrooniline kommunikatsioon) kuuluvad tööandja intellektuaalomandi alla ning töötaja loovutab kõik oma autoriõigused tööandjale. Samuti tuleks ettevõtetes kehtestada sisereeglistik, mis näeb ette eri liiki dokumentide säilitamise tähtsajad ning tähtsaja möödudes hävitamise korra. Võttes arvesse, et tegemist on isikuandmeid sisaldavate dokumentidega, paneb säilitamistähtaegade määramise kohustuse vastutavale andmetöötlejale ka GDPR art 5

---

<sup>144</sup> Euroopa Andmekaitseasutuste töögrupp on mitmel juhul jõudnud järeldusele, et IP-aadressid kvalifitseeruvad isikuandmeteks. Nt Arvamus 4/2007 isikuandmete mõiste kohta; Arvamus 1/2008, mis käsitleb andmekaitse küsimusi seoses otsingumootoriga

<sup>145</sup> AKI juhendmaterjal. IP-aadress ja privaatsus. 07.12.2016. Kättesaadav: [http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/ip\\_ja\\_privatsus.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ip_ja_privatsus.pdf) 03.04.2017

<sup>146</sup> sama, lk 3

<sup>147</sup> Euroopa Kohtu 19.10.2016.a otsus C-582/14 *Breyer vs Saksamaa* p 49

<sup>148</sup> sama p 47

Ig 1e ning uue IKS-i § 16. Kui mitte arvestada seadusega ette nähtud dokumentide (raamatupidamisdokumendid, lepingud, töösuhtega seonduv dokumentatsioon) säilitamise tähtaegu, võiks magistritöö autori hinnangul tavapärase olulise töödokumendi säilitamise maksimaalseks kestuseks olla 10 aastat selle loomisest.

### 3.5. Eriliigilised isikuandmed töösuhtes

Varemkehtinud IKS § 4 Ig-st 2 on delikaatsed isikuandmed poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi kirjeldavad andmed, välja arvatud andmed seadusega ettenähtud korras registreeritud eraõiguslike juriidiliste isikute liikmeks olemise kohta; etnilist päritolu ja rassilist kuuluvust kirjeldavad andmed; andmed tervises seisundi või puude kohta; andmed pärilikkuse informatsiooni kohta; biomeetrilised andmed (eelkõige sõrmejäljepeopesajälje- ja silmairiisekujutis ning geenandmed); andmed seksuaalelu kohta; andmed ametiühingu liikmelisuse kohta; andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.

Delikaatsete andmete asemel kasutab GDPRi artikkel 9 eriliigiliste isikuandmete mõistet. Artikli esimene lõige keelab selliste isikuandmete töötlemise, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, samuti on keelatud töödelda geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmeid, terviseandmeid või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta. Võrreldes varemkehtinud IKS-i määratlusega, on GDPRi loetelust seega välja jäänud üksnes kriminaalmenetluses osalemist puudutavad andmed ning millised on reguleeritud eraldi direktiiviga.<sup>149</sup>

Eriliigiliste isikuandmete töötlemine GDPR-i alusel on lubatud mh nt andmesubjekti nõusolekul; vastavat töötlemist õigustava juriidilise kohustuse olemasolu korral; andmesubjekti või teiste isikute eluliste huvide kaitseks; avalike huvide kaitseks ja

---

<sup>149</sup> 27.04.2016 Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2016/680 mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist

rahvatervise kaitseks.<sup>150</sup> Uue IKS-i §-s 19 on välja toodud, et eriliiki isikuandmete töötlemine on lubatud üksnes juhul, kui see on rangelt vajalik ning üksnes siis kui töötlemise lubatavus on sätestatud õigusaktis või kui see on vajalik andmesubjekti või teise füüsilise isiku eluliste huvide kaitseks või töödeldakse selliseid isikuandmeid, mida andmesubjekt on ilmselgelt avaldanud.

Seega rõhutatakse, et eriliigilised isikuandmed peavad olema töösuhte olemusest tööandjale vajalikud, st nende töötlemisel peab olema mingisugune tööandja huve teeniv eesmärk. Näiteks on AKI ühe sellise vajaduse all silmas pidanud töökohas organiseeritavaid sotsiaalseid tegevusi.<sup>151</sup>

Kui mõningatel ootamatutel juhtudel võib olla töötaja terviseandmete töötlemine ilma tema nõusolekuta GDPR art 9 lg 2c alusel töötaja enda, tööandja, teiste töötajate või kolmandate isikute (nt klientide) elu või tervise kaitseks olla lubatud, näiteks olukorras, kus töötaja haigestub ootamatult ja tõsiselt ning talle on vaja kutsuda kiirabi, siis teatud delikaatsete isikuandmete töötlemise osas kehtib tööandjale aga absoluutne keeld. Näiteks sedastab Inimgeeniuringute seaduse<sup>152</sup> § 26 lg 1, et tööandjal on keelatud koguda geneetilisi isikuandmeid töötaja kohta ning nõuda töötajalt koeproovi või DNA kirjelduse andmist.

Eriliigilistest isikuandmetest on nii Soome asjakohane seadus,<sup>153</sup> kui Ühendkuningriigi andmekaitseasutuse juhend<sup>154</sup> pidanud vajalikuks eraldi käsitleda töötaja terviseandmeid (sh töötervishoid ja tervisekontroll töökohal), narkootiliste- ja psühhotroopsete ainete kasutamise (ingl. k *drug use*) kontrollimist ja rõhutavad, et keelatud on geneetiliste uuringutega (ingl.k *genetic/ generic testing*) seonduvate andmete nõudmine ning geneetilise materjali kogumine. Soome seaduses on väga konkreetselt piiratud ka isikute ringi, kellel on õigus töötaja terviseandmeid töödelda.<sup>155</sup> Samalaadse soovitusena töötlemiseks õigustatud isikute ringi

---

<sup>150</sup> Täielik loetelu GDPR art 9 lg 2

<sup>151</sup> AKI juhendmaterjal lk 43

<sup>152</sup> Inimgeeniuringute seadus – RT I 14.03.2014, 30

<sup>153</sup> *Laki yksityisyyden suojasta työelämässä* § 2 lg 5, § 3 ja § 4

<sup>154</sup> *Information Commissioner's Office. The Employment Practices Code*, lk 79-94

<sup>155</sup> Vastavalt *Laki yksityisyyden suojasta työelämässä* § 2 lg 5 p-le 2 on õigustatud isikuteks üksnes need, kes valmistavad ette või võtavad vastu töösuhtega seonduvaid otsuseid. Sellisteks isikuteks võiks magistritöö autori hinnangul lugeda näiteks personalitöötajat, raamatupidajat, kes tegeleb ka personalitööga ning ettevõtte juhtkonda.

piiramiseks annab ka Ühendkuningriigi juhend.<sup>156</sup>

Eesti tööõiguses tuleb terviseandmete töötlemist taaskord sisustada läbi mitme erineva õigusakti. Näiteks on töötervishoiu ja tööohutuse seaduse (TTOS) § 19<sup>2</sup> lg 1 p 3 kohaselt on ettevõtte juhtkonnal õigus saada töötervishoiuspetsialistilt töötaja kohta ainult hinnang piirangute vajalikkuse osas, kuid mitte andmeid analüüside tulemuste ega muude meditsiiniliste andmete kohta. See tekitab hulga küsimusi teatud töökohtadel läbiviidavate joobe- ja/või narkokontrollide ning nende tulemuste säilitamise õiguspärasuse osas ning samuti ka kõikvõimalike meditsiiniliste tõendite nõudmise osas ning samaaegselt ka riskidest, mida tööandjal tuleb kanda.

### 3.5.1. Ajutine töövõimetus

Kehtiva õiguse kohaselt on töötajal on ajutise töövõimetus tõttu õigus töötamisest keelduda kahel alusel. TLS § 42 võimaldab töötajal nõuda mõistlikus ulatuses vaba aega juhul, kui eksisteerib tema isikust tulenev põhjus, miks ta ei saa tööd teha või kui temalt ei saa töö tegemist oodata muul tema isikust mittetuleneval põhjusel. Vastavalt TLS §-le 38 peab tööandja maksma töötajale selle aja eest siiski keskmist töötasu. Seejuures ei tohi töötaja olla ise tahtlikult või raske hooletuse läbi põhjustanud olukorda, miks ta ei saa ajutiselt tööd teha.

TLS seletuskirjas on sellisteks töötaja isikust tulenevateks põhjusteks välja toodud notari või arsti vastuvõtul käimist, samuti ka lähedase matust. Täiendavalt on selgitatud, et juhul, kui töötaja sellised „ärakäimised“ muutuvad pikemaajalisteks või igapäevasteks (näiteks regulaarsetel meditsiiniprotseduuridel käimine, haige vanema eest hoolitsemine, lapsel koolis järelkäimine jms) tööandjal töötasu maksmise kohustust siiski ei ole ning leida tuleb muu pooli rahuldav kokkulepe.<sup>157</sup>

Eelpool väljatoodud õigustatud isiklike põhjuste puhul ei ole töötajal seadusest tulenevat kohustust oma eemalviibimist tööandjale tõendada. Siiski on paljud tööandjad, lähtudes

---

<sup>156</sup> *Information Commissioner's Office. The Employment Practices Code*, lk 85

<sup>157</sup> TLS seletuskiri lk 38

kontrollprintsibist<sup>158</sup> praktikas võtnud suuna sellele, et töötajal tuleb töölt äraolekut asjakohaselt põhjendada, esitades tööandjale arstitõendeid arsti vastuvõtul käimise kohta, olgu tegemist siis hambaarsti, günekoloogi või psühhiaatriga.<sup>159</sup>

Ühest küljest võimaldab TLS § 15 lg 2 p 8 tööandjatel nõuda töötajalt välja selliseid andmeid, mille vastu on tööandjal õigustatud huvi ning kahtlemata võib pidada õigustatuks tööandja huvi selle kohta, miks tema töötaja tööajal mujal viibis.

Soome tööseaduses on töölt eemalolek lubatud „kaalukatel perekondlikel põhjustel“<sup>160</sup> ning „pereliikme või lähedase eest hoolitsemiseks“<sup>161</sup> ning lisaks tööandja teavitamisele on töötaja kohustatud tööandja nõudmisel esitama ka „piisava ja usaldusväärse tõendi“. Seega on töötaja isikust tulenev töölt eemalviibimine reguleeritud üsna ühetaoliselt. Siiski tekib küsimus viidatud „tõendi“ osas. Millega piisavalt ja usaldusväärset tõendada näiteks lähedase matusel käiku?

Andmekaitse Inspektsioon on aga välja toonud, et tööandjal pole nagunii objektiivselt võimalik kindlaks teha kõiki TLS §-s 38 sedastatud eeldusi, mh ka seda, kas töötaja arstile pöördumise põhjuseks on tema enda poolt tahtlikult tekitatud vigastus või elektriku kutsumise vajaduse tingis töötaja enda poolt valesti ühendatud juhmestik.<sup>162</sup>

Ühest küljest on tegemist liigse sekkumisega töötaja privaatsusesse ning asjaolu, et töötaja viibis tööajast näiteks hambaarsti juures, ei ole magistritöö autori hinnangul käsitletav niisuguse asjaoluna, mille puhul oleks töösuhte normaalseks ning tõrgeteta toimiseks arstitõend hädavajalik ning seega riive töötaja põhiõigustesse lubatud. Teisest küljest lasub tööandjal tulenevalt TTOS-ist tööõnnetuste ja kutsehaigestumiste põhjustamisest kahju hüvitamise kohustus ning selle vältimiseks peab tööandja olema valmis tõendama, et ei ole kahju põhjustamises süüdi. Seega teeniks erinevate tervisetõendite säilitamine kahtlemata tööandja huve. Uue IKS-i § 19 lg 1 näeb ette, et eriliigiliste andmete töötlemine peab olema rangelt vajalik. Seega võiks tervisetõendite säilitamine tulevaste võimalike

---

<sup>158</sup> TLS § 1 lg 1 – töötaja allub tööandja kontrollile

<sup>159</sup> AKI juhendmaterjal lk 45

<sup>160</sup> *Työsopimuslaki* § 4 lg 7

<sup>161</sup> sama § 4 lg 7a

<sup>162</sup> AKI juhendmaterjal lk 45

kutsehaigestumistega seonduvate vaidluste tarbeks olla õiguspärane juhul, kui kutsehaigestumise tõenäosus on suur, nt sellistes töökeskondades, kus töötaja puutub igapäevaselt kokku kemikaalide, mikroorganismide, füüsikaliste ohutegurite vms-ga.

Teine ajutise töövõimetuse põhjus on töötaja tervis. TLS § 19 p 2 kohaselt on töötajal õigus keelduda töö tegemisest, kui ta on ajutiselt töövõimetu Ravikindlusseaduse tähenduses. Töövõimetuse tuvastab arst, hambaarst või ämmaemand ning väljastab selle kohta töövõimetuslehe.<sup>163</sup> Ajutise töövõimetuslehe liigid on: haigusleht, hooldusleht, sünnitusleht ja lapsendamisleht.<sup>164</sup>

TLS § 15 p 10 näeb ette, et töötaja peab tööandjale esimesel võimalusel teatama oma ajutisest töövõimetusest ja võimaluse korral selle eelduslikust kestusest. Siiski ei pea töötaja tööandjat teavitama töövõimetuslehe täpsematest asjaoludest sh ka sellest, mis töövõimetuse põhjustas. Selliseid detaile ei märgita ka töövõimetuslehele, mistõttu võib praktikas ette tulla juhtumeid, kus tööandja ei usalda töötaja poolt esitatud töövõimetuslehte ning arvavad, et töötajad kasutavad tervislikke põhjuseid ettekäändena, et saada puhkust, mida tööandja ei võimaldanud.<sup>165</sup>

Kuivõrd töövõimetuslehe väljaandmise õigus on meditsiinilist pädevust omaval isikul, siis ei ole tööandjal isegi olukorras, kus ilmneb, et töötaja on töövõimetuslehe ajal käinud näiteks soojamaareisil, õigust iseseisvalt otsustada, et töövõimetuslehe väljaandmine oli põhjendamatu. Tulenevalt TTOS §-st 12<sup>1</sup> on töövõimetusleht tööandjale aluseks haigushüvitise maksmiseks, kuid tööandja ei pea haigushüvitist töötajale maksma, kui esinevad RaKS §-s 60 sätestatud juhud, milleks muuhulgas on olukorrad, kus haigestumise või vigastuse põhjustas isiku tahtlus; haigestumine või vigastus on tingitud liiklusseaduse alusel kehtestatud korras või arsti tehtud ekspertiisiga tuvastatud joobeseisundist; isik eirab arsti määratud meditsiiniliselt põhjendatud ravi, mille tõttu on tervenemine takistatud;<sup>166</sup> Samad hüvitisest keeldumise alused kehtivad ka Eesti Haigekassale.

Tulenevalt VÕS §-st 770 vastutab tervishoiuteenuse osutaja patsiendile õige diagnoosi

<sup>163</sup> Ravikindlustuse seadus (RaKS) § 52 lg 2 – RT I 27.12.2016, 12

<sup>164</sup> RaKS § 52 lg 3

<sup>165</sup> AKI juhendmaterjal lk 45

<sup>166</sup> RaKS § 60 lg 1 pp 1-3



määramise eest. Sellest tulenevalt vastutab töövõimetuslehe põhjendatuse ja kindlustusjuhtumi määramise eest samuti töövõimetuslehe väljastanud arst, hambaarst või ämmaemand. Andmekaitse Inspektsiooni arupärimisele vastates leidis Eesti Haigekassa siiski, et kahtluse korral on tööandjal õigus pöörduda haigekassa piirkondlikule osakonnale avaldus haiguslehe väljaandmisega seotud asjaolude kontrollimiseks.<sup>167</sup> Vastavalt AKI seisukohale, on tööandjal õigus eelnimetatud kontrolli tulemustest teada saada, kas töövõimetuslehe väljastamine oli põhjendatud või mitte ning kas tuvastati hüvitise maksmisest keeldumise alus.<sup>168</sup> Isikuandmete töötlemine toimub sellisel juhul GDPR art 9 lg 2b alusel, sest tööandja töötleb töövõimetuslehega seonduvaid isikuandmeid seadusega ettenähtud ülesande täitmiseks, milliseks on TTOS §-st 12<sup>1</sup> tulenev kohustus maksta haigushüvitist. Siiski tuleb silmas pidada, et tööandjal on õigus nõuda üksnes kontrolli tulemusi ning mitte töötaja detailset haiguslugu, sh arsti soovitusi ravirežiimi osas.

### 3.5.2 Tervisekontroll töökohal

Töötajate tervisekontroll on nõutav selliste töötajate puhul, kelle tervist võib tööprotsessi käigus mõjutada töökeskkonna ohutegur või töö laad.<sup>169</sup> Tervisekontrolli läbiviimise kord on eraldi fikseeritud vastava Sotsiaalministri määrusega,<sup>170</sup> mille lisas 1 on välja toodud ohutegurite ka töö ohtliku laadi avatud loetelu, kus muuhulgas sedastatakse öötöö ja ka kuvariga töötamine. Teatud elualade puhul on vastavalt Nakkushaiguste ennetamise seadusele nõutav ka nakkushaiguste (sh kopsuröntgeni tegemine) korraline kontrollimine.<sup>171</sup>

Magistritöö teemat silmas pidades, on oluline rõhutada, et tööandjal ei ole õigust nõuda ei töötervishoiuarstilt ega töötajalt endalt tervisekontrolli tulemusi. Tulenevalt TTOS § 19<sup>2</sup> lg 1 p 2 ja 3 kohaselt tagab töötervishoiuspetsialist töötajate tervise- ja eraeluandmete konfidentsiaalsuse ning teatab tervisekontrolli tulemustest ettevõtte juhtkonnale ainult seda, millised piirangud on töötajale tööülesannete täitmiseks seatud tervise vastunäidustuste tõttu.

---

<sup>167</sup> AKI juhendmaterjal lk 46

<sup>168</sup> AKI juhendmaterjal lk 46

<sup>169</sup> Töötervishoiu ja tööohutuse seadus (TTOS) § 13 lg 1 p 7 – RT I 08.07.2016, 39

<sup>170</sup> Sotsiaalministri 24.04.2003. a määrus nr 74 “Töötajate tervisekontrolli kord” - RT I, 10.04.2015, 3

<sup>171</sup> Nakkushaiguste ennetamise ja tõrje seadus § 24 – RT I 04.12.2015, 3

Analoogselt on töötajate tervise kontrollimine lahendatud Soomeski. Kui Eestis tähendab tervisekontrolli valdavalt töötajate füüsilise kontrollimist, siis Soomes võib kõne alla tulla ka töötaja isiksuse ja sobivuse (ehk sisuliselt vaimse tervise) hindamine vastava ala spetsialistide poolt.<sup>172</sup>

Kuivõrd lisaks tervisekontrolli korraldamisele kohustub tööandja selle eest ka tasuma,<sup>173</sup> tekitab see praktikas kulude kokkuhoiu eesmärgil sageli küsimusi, kas tööandjal võiks seetõttu olla õigus määrata või piirata, milliseid uuringuid ja analüüse töötajale tervisekontrolli raames teha. Näiteks, kas on lubatud kontoritöötaja puhul tema saatmine üksnes silmakontrolli?

Tulenevalt Tervisekontrolli korra § 5 lg-st 4 määrab töötervishoiuarst olles tutvunud tervisekontrolli alusdokumentide ning töökohal töötaja töökeskkonna ja töökorraldusega, vajalikud terviseuuringud, kaasates vajadusel eriarste. Seega pelgalt silmakontrolli saatmine kokkuhoiu eesmärgil ei vabasta tööandjat täieliku tervisekontrolli korraldamise kohustusest. Töötaja tervisekontroll algab esmase tervisekontrolliga tööle asumise esimese kuu jooksul ning edaspidi töötervishoiuarsti näidatud ajavahemiku järel, kuid mitte harvem kui üks kord kolme aasta jooksul ning alaealise töötaja puhul mitte harvem kui üks kord kahe aasta jooksul.<sup>174</sup>

### 3.4.3. Joobeseisund töökohal

Käesolevas alapeatükis käsitletakse joobeseisundina nii alkoholi- kui narkootiliste ja psühhotroopsete vms ainete mõju all olemist. Õiguslikult kuulub joobeseisund terviseandmete hulka,<sup>175</sup> millised loetakse vastavalt GDPR art 9 lg-le 1 eriliigilisteks isikuandmeteks. Seega on nii isiku joobeseisund kui selline ning ka selle tuvastamine käsitletavad eriliigiliste isikuandmete töötlemisena.

Huvitaval kombel kõneleb Soome privaatsust töökohal puudutav õigusakt üksnes

<sup>172</sup> *Laki yksityisyyden suojasta työelämässä* § 4 lg 13

<sup>173</sup> TTOS § 13 lg 1 p 7

<sup>174</sup> Sotsiaalministri 24.04.2003. a määrus nr 74 "Töötajate tervisekontrolli kord" § 5 lg 2

<sup>175</sup> RKHKo 3-3-1-98-06 p 22. 17.04.2007

narkotestidest ja seda nii töösuhte ajal, kui ka juba värbamisel.<sup>176</sup> Täpsemalt reguleerib viidatud narkotestide läbi viimise korda Soome töötervishoiuseadus, milles samuti käsitletakse just „narkootilisi aineid“ (soome k. *huumausaine*).<sup>177</sup> Alkoholi joobes töötaja osas on Soome seadusandlus puudulik.

Joobes töötaja võib põhjustada tõsist ohtu nii iseenda, kui teiste isikute tervisele ja ka elule,<sup>178</sup> mistõttu on üheks tööandja põhikohustuseks töötervishoiu ja tööohutuse nõuetele vastavate töötingimuste tagamine töökohal.<sup>179</sup> Muuhulgas sisustab seda ka TTOS § 13 lg 1 p-st 15 tulenev kohustus alkoholi-, narkootilises või toksilises joobes või psühhotroopse aine mõju all olev töötaja töölt kõrvaldada. Vastust sellele, mida defineerida joobe all ning kuidas peaks tööandja korraldama joobe tuvastamise, fikseerimise ning töötaja eemaldamise TTOS ei anna.

Riigikohtu halduskolleegium on seisukohal, et mõiste "joobnuna" all võib mõista alkoholi tarvitamisest põhjustatud terviseseisundit, mis avaldub väliselt tajutavates häiritud või muutunud kehalistes või psüühilistes funktsioonides ja reaktsioonides.<sup>180</sup> Samuti on kohus märkinud, et joobnud oleku tuvastamine ei eelda kindlat alkoholikontsentratsiooni veres ega väljahingatavas õhus, vaid eelkõige just selle tuvastamist, et isiku kehalised või psüühilised funktsioonid on alkoholi tarvitamise tagajärjel muutunud või häirunud.<sup>181</sup> Analoogia korras võib magistritöö autori hinnangul tõlgendust kasutada ka narkootiliste või psühhotroopsete ainete tarbimisest tekkinud joobe tuvastamiseks.

Korralduseadus (KorS) § 36 lg 1 defineerib joobeseisundina alkoholi, narkootilise või psühhotroopse aine või muu joovastava aine tarvitamisest põhjustatud terviseseisund, mis avaldub väliselt tajutavas häiritud või muutunud kehalistes või psüühilistes funktsioonides ja reaktsioonides. Samuti sedastab KorS võrdlemisi põhjaliku käitumisjuhise joobe tuvastamiseks ning kainenemiseni kinnipidamiseks (avalikust ruumist eemaldamiseks).<sup>182</sup> Probleem väljendub aga selles, et KorS reguleerib üksnes avalikus ruumis toimuvat ning

---

<sup>176</sup> *Laki yksityisyyden suojasta työelämässä* § 3 lg 6 ja 7

<sup>177</sup> *Työterveysluotolaki* § 4 lg 19

<sup>178</sup> Autori märkus: näiteks politsei- ja piirivalve teenistujad, meditsiinitöötajad, lastega tegelevad töötajad, tootmistöölised jne

<sup>179</sup> TLS § 28 lg 2 p 6

<sup>180</sup> RKKHo nr 3-3-1-45-11 p. 11. 26.10.2011

<sup>181</sup> sama p. 13

<sup>182</sup> Korralduseadus (KorS) § 37 jj – RT I 02.12.2016, 6

defineerib avaliku ruumina määratlemata isikute ringile kasutamiseks antud või määratlemata isikute ringi kasutuses olev maa-ala, ehitis, ruum või selle osa, samuti ühissõiduk.<sup>183</sup> Eraõiguslik töökoht kui selline ei ole aga KorS-i mõttes avaliku kohana alati käsitletav (erandina võiks kõne alla tulla näiteks kaupluse müügisaalid vms, kuhu kolmandad isikud piiramatult ligi pääsevad). Avalikku korra rikkumise võimalikkust töökohal on iseenesest kinnitanud ka Riigikohus, seda küll üsna ammusel lahendis.<sup>184</sup>

Tänases praktikas on tööandjad kasutanud joobe tuvastamisel kasutanud politsei abi, kes tuvastab alkoholi ja narkootilist joovet juhtudel, milleks loetakse muuhulgas sõidukijuhi või muu isiku, kui on alust kahtlustada, et isik on toime pannud süüteo, mille koosseisuliseks tunnuseks on joobeseisund, alkoholipiirmäära ületamine või narkootilise või psühhotroopse aine või muu sarnase toimega aine tarvitamine.<sup>185</sup> Siiski võib magistritöö autori hinnangul tõusetada küsimus, kui mõistlik võiks olla niivõrd oluliste avalike ressursside kasutamine ühe napsitanud töötaja seisundi fikseerimiseks ning teine teema selles, et kuna üldjuhul ei ole eraõiguslik töökoht samastatav avaliku kohana, siis politseil puudub ka kohustus kutsungile reageerida, eeldades, et kellegi elu või tervis ohus ei ole. Seega sisuliselt, kuigi TTOS-i kohustab tööandjat joobes töötaja töökohalt eemaldama, siis tegelikkuses puudub eraõiguslike töösuhete puhul seadusest tulenev alus joobe tuvastamiseks, selle kontrollimiseks ja olukorra fikseerimiseks.

Tööandjal on lubatud eriliigilisi isikuandmeid töödelda kas andmesubjekti nõusolekul või õigusaktides sätestatud alusel. Seega iseenesest oleks tööandjal võimalik teha joobekahtlusega töötajale ettepanek näiteks alkomeetrisse puhumiseks või ka arsti juurde pöördumiseks, kuid on oluline rõhutada, et tööandja ei saa töötajat selleks sundida. Samuti on alkomeetrist kasu üksnes alkoholi joobe tuvastamiseks ning näidu hilisem tõendamine (näiteks kohtumenetluse käigus) võib olla raskendatud. Andmekaitse Inspeksioon taunib ka nõ tunnistajate kasutamist joobekahtluse kindlaks tegemiseks, kuivõrd tööandjal ei ole õigust levitada (joobes) töötaja kohta delikaatseid isikuandmeid.<sup>186</sup> Küll aga leiab AKI, et kasutada saab neid isikuid, kes on ilma tööandja sellekohase pöördumiseta teinud ise tähelepanekuid

---

<sup>183</sup> KorS § 54 lg 1

<sup>184</sup> RKKKo nr 3-1-1-134-96. 10.12.1996

<sup>185</sup> AKI juhendmaterjal lk 46

<sup>186</sup> sama

kaastöötaja suhtes.<sup>187</sup> Õiguslikult selline alus siiski puudub.

Ühe võimalusena võiks töötaja õigust ebaadekvaatses seisundis oleva kaastöötaja kohta osas tööandjale vihje andmist sisustada läbi TLS § 15 lg 1 p-i 8, mille kohaselt on tööandjal õigus nõuda töötajalt andmeid kõigist töösuhtega seonduvatest olulistest asjaoludest, mille vastu tööandjal on õigustatud huvi. Kuna TTOS paneb tööandjale selgesõnalise kohustuse ohutu töökeskkonna tagamiseks (sh joobes töötaja eemaldamiseks), siis võiks iseenesest olla tööandja huvides teada, et keegi tema töötajatest on töökohal purjus. Samas takerdub arutlus siiski eriliigiliste isikuandmete töötlemise taha, mille osas tähelepanelikul töötajal puudub igasugune õigus, seega on magistritöö autori hinnangul joobe tuvastamisel kaastöötajate avaldustele tuginemine või nende alusel tegutsemine ebaõige ning eelduslikult peaks tööandja töötamist korraldama selliselt, et temal endal oleks ülevaade oma töötajatest.

GDPR-is on terviseandmete töötlemine muu hulgas lubatud juhul kui töötlemine on vajalik seoses vastutava töötleja või andmesubjekti tööõigusest ning sotsiaalkindlustuse ja sotsiaalkaitse valdkonna õigusest tulenevate kohustuste ja eriõigustega niivõrd, kuivõrd see on lubatud liidu või liikmesriigi õigusega või liikmesriigi õiguse kohase kollektiivlepinguga, millega kehtestatakse asjakohased kaitsemeetmed andmesubjekti põhiõiguste ja huvide kaitseks.<sup>188</sup> Uue IKS-i § 19 lg 1 kohaselt on eriliiki isikuandmete töötlemine lubatud, kui see on rangelt vajalik ja vastav õigus on kehtestatud seadusega või töötlemine on vajalik andmesubjekti või teiste isikute eluliste huvide kaitseks või töödeldakse andmeid, mida andmesubjekt on ilmselgelt juba avaldanud.

Nagu eelpool viidatud on tööandjal kohustus oma töötajatele tagada ohutu töökeskkond<sup>189</sup> ning vastavalt TTOS § 13 lg 1 p-le 15 tuleb tööandjal alkoholi-, narkootilises või toksilises joobes või psühhotroopse aine mõju all olev töötaja töölt kõrvaldada. TTOS § 13 lg 2 kohaselt võib tööandja kehtestada ettevõttes seadusega võrreldes rangemad töötervishoiu ja tööohutuse nõuded ning kontrollida ka nende täitmist. Seega on olemas siseriiklikust tööõiguse ja sotsiaalkaitse valdkonnast tulenevad normid, mille järgmiseks on vajalik terviseandmete töötlemine. Eeltoodut arvesse võttes, leiab käesoleva magistritöö autor, et

---

<sup>187</sup> AKI juhendmaterjal lk 47

<sup>188</sup> GDPR art 9 lg 2 b

<sup>189</sup> TLS § 28 lg 2 p 6

tööandjal on põhimõtteline õigus joobekahtlusega isiku puhul nõuda joobe tuvastamist, kas politsei või meditsiinitöötaja kaasabil ning tegevuse tulemuse kohta vastava kirjaliku akti koostamist ka juhul, kui töötaja indikaatorvahendi kasutamisest keeldus.

Kuivõrd joobe defineerimine ja tuvastamine on tänases praktikas raskendatud, soovitab magistr töö autor eeltoodule tuginedes tööandjatel töökohal kehtestada töölepingu lahutamatu osana sisekorra eeskirjad,<sup>190</sup> mis muuhulgas annavad ette ka täpse käitumisjuhendi joobekahtlusega töötajaga tegelemiseks ning eraldi peaks olema välja toodud töötaja nõusolek joobekahtluse korral vastava kontrolli läbiviimiseks ja töötaja töölt eemaldamiseks. Sisekorda peab olema töötajale allkirja vastu tutvustatud ning on oluline, et tööandja ka ise oma reeglite järgi tegutseks. Sellisel juhul on kõigile osapooltele juba ette teada, kuidas toimida ning milliseid tagajärgi võib joobeseisundis töökohal viibimine põhjustada.

Riigikohus on märkinud, et joobeseisundi tõendamine on samastatav tavapärase faktilise asjaolu tõendamisega.<sup>191</sup> Samuti on praktikas avaldatud, et indikaatorvahendi näidu kasutamine (teenistus)vaidluses tõendina ei sõltu sellest, kas isik oli näiduga nõustunud või mitte, vaid vastavas menetluses kehtestatud tõendi lubatavuse reeglitest.<sup>192</sup> Seega, kui töökohal on kehtestatud konkreetne ja selge käitumisjuhised, mida on töötajale eelnevalt tutvustatud ning temalt on võetud nõusolek joobekahtluse korral tervise seisundi tuvastamiseks (ja seda ei ole tagasi võetud), on magistr töö autori hinnangul tegemist õiguspärase tõendi kogumisega,<sup>193</sup> mis oleks kasutatav nii tsiviil- kui halduskohtumenetluses.

#### 3.5.4. Biomeetrilised andmed

Käesoleva magistr töö üheks ülesandeks on läheneda privaatsuse ja isikuandmete temaatikale ka tulevikkuvaatavalt ning seetõttu käsitletakse biomeetriat käesolevas alapeatükis mõnevõrra hüpoteetilises võtmes.

---

<sup>190</sup> Avalikus teenistuses reguleerib vastavat õigust ATS § 67

<sup>191</sup> RKHKo nr 3-3-1-45-11 p. 12. 26.10.2011.

<sup>192</sup> RKHKo nr 3-3-1-13-16 p. 12. 18.10.2016

<sup>193</sup> Tsiviilkohtumenetluses sätestab tõendi lubatavuse alused TsMS § 238; vastavalt halduskohtumenetluse seadustiku § 56 lg-le 2 kohadatakse haldusmenetluses tõendite lubatavusele tsiviilkohtumenetluse sätteid.

Biomeetrilised andmed on mitmesugused bioloogilised, füüsilised, psühholoogilised, käitumuslikud või sarnased omadused, mida kasutatakse isiku või isikusamasuse tuvastamisel.<sup>194</sup>

GDPR art 4 lg 14 loetleb biomeetriliste andmetena konkreetse tehnilise töötlemise abil saadavaid isikuandmeid isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed;

Tänases Eesti praktikas on biomeetrilised isikutuvastusvahendid laialdaselt kasutuses piiripunktides (sh lennujaamad, sadamad) sisejulgeoleku tagamiseks, kuid ettevõtetes ja asutustes leiavad need rakendust äärmiselt vähe<sup>195</sup> ning valdavalt eelistatakse tööandja territooriumile pääsemiseks, sellel liikumiseks ja ka oma tööjaama sisselogimiseks erinevaid kiipkaarte, koode ja paroole. Ühe võimalusena võiks tehnoloogia arenedes ning turvalisuse tõstmiseks kõne alla tulla nende asendamine biomeetriliste vahenditega.

Vastavalt AKI seisukohale<sup>196</sup> sõltub biomeetriliste andmete töötlemise lubatavus eelkõige andmeid töötleva süsteemi tehnoloogiast. Sellest tulenevalt võib sellised süsteemid liigitada kahte kategooriasse:

1) süsteemid, mis salvestavad biomeetrilise jäljendi (näiteks silmaiirisekujutise või sõrmejälje); 2) süsteemid, mis loovad biomeetrilise jäljendi alusel koodi, jäljendit ennast ei salvestata. Selliseid süsteeme on omakorda kolme liiki: (a) kood salvestatakse kesksesse andmebaasi; (b) kood salvestatakse seadmesse; (c) kood salvestatakse kaasaskantavale andmekandjale, nt kiipkaardile.

Süsteem, mis salvestab endasse biomeetrilist jäljendit, töötleb selgelt delikaatseid isikuandmeid, seega muutub ka tööandja automaatselt delikaatsete isikuandmete töötlejaks. Kehtvatest õigusaktidest ei tulene tööandjale õigust isikuandmeid töödelda tööandja

---

<sup>194</sup> Prof. Marcel Yon'i tõlgendus. AKI juhend biomeetriliste isikuandmete töötlemise kohta. Arvutivõrgus: [http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/Biomeetriliste%20isikuandmete%20%C3%B6tlemine.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Biomeetriliste%20isikuandmete%20%C3%B6tlemine.pdf) 23.03.2017

<sup>195</sup> Autori märkus: on teada selliseid ettevõtteid/ asutusi, kus kasutatakse nn 2FA ehk kahe faasilist autentimist, mille puhul ettevõtte territooriumil liikumiseks kasutakse kiipkaarti või uksekoodi ning piiratud ligipääsuga ruumidesse sissepääsuks (nt arhiivid, serveriruumid jms) sõrmejälgi või nende alusel genereeritavaid täiendavaid koode.

<sup>196</sup> AKI juhendmaterjal lk 54

territoriumile või infosüsteemidele ligipääsemise õiguse kontrollimiseks, samuti on Inimgeeniuringute seaduse § 26 lg 1 tööandjatel keelatud töötajatelt geneetilise materjali nõudmine või talletamine, seega saab ka biomeetriliste andmete töötlemine kõne alla tulla üksnes kas töötaja sellekohasel nõusolekul või lepingu täitmise eesmärgil, kui lepingus on eraldi toodud tingimused, mille alusel tööandja territooriumile, ruumidesse või infosüsteemidesse pääseb.<sup>197</sup>

Biomeetrilise jäljendi salvestamise asemel peetakse turvalisemaks ning ka andmekaitse nõuetega rohkem kooskõlas olevaks süsteeme, mis loovad biomeetria abil üksnes ligipääsuks vajaliku koodi, kuid biomeetrilisi andmeid kuidagi ei säilitata. Analoogsed süsteemid on ka nutiseadmete puhul väga laialdaselt kasutuses.<sup>198</sup>

Ka AKI soovitab eelistada selliseid süsteeme, kus biomeetria abil loodav kood jääks kasutaja (töötaja) enda valdusesse.<sup>199</sup> Magistritöö autori hinnangul on sellise süsteemina käsitletav näiteks sõrmejäljelugejaga (töö)telefon, mis faktiliselt kuulub küll tööandjale, kuid igapäevaselt on töötaja valduses. Tööandja territooriumil liikumiseks genereeritakse igakordselt uus kood, mistõttu ei saa ka tekkida olukorda, kus tööandja või keegi kolmas saaks töötaja personaalseid koode kasutada. Üheks negatiivseks asjaoluks võiks välja tuua kasutusmugavuse – andmeid säilitava süsteemi puhul piisab ühest statsionaarsest seadmest, biomeetriaal töötava koodigeneraatori puhul on vaja mitut seadet. Seega on tööandja otsustada, kas valida mugavus või isikuandmete töötlemisest tekkivad ohud.

### 3.6. Kaugtöö

Magistritöö autor leiab, et klassikalise töösuhte käsitus on mõnevõrra aegunud ega ole enam alati kohaldatav, kuivõrd range alluvussuhe on muutunud pigem partnerluseks. Tänapäevases oludes on töötaja oma intellektuaalsete võimete ja kogemuste poolest tööandjast sageli üle, eriti näiteks IKT valdkonnas. See omakorda tingib selle, et jõu- ja võimupositsioonid on vahetumas - häid spetsialiste on keeruline leida ja töötingimuste läbirääkimiste laua taga on töötajal

---

<sup>197</sup> AKI juhendmaterjal lk 54

<sup>198</sup> Süld, R. Biomeetrilise isikutuvastuse levik muudab kogu ühiskonda. Postimees 03.06.2016.

<sup>199</sup> AKI juhendmaterjal lk 55



kahtlemata suuremad võimalused oma õigusi paika panna, kui varasemalt.

Asjaolu, et töötajad on muutumas üha iseseisvamaks, toetab ka kaugtöö kontseptsioon, mida propageeritakse muuhulgas tööandja kulude kokkuhoiu, töötajate motiveerimise, maapiirkondade elustamiseks ja puuetega inimeste tööellu aktiivsemaks kaasamiseks.<sup>200</sup>

Eesti Rakendusuuringu Keskuse Centar poolt 2009. aastal läbi viidud uuringus leiti, et organisatsioonides pole tänasel päeval teemaks mitte niivõrd see, kas kaugtöö kasutamist lubada vaid see, kuidas korraldada kaugtööd selliselt, et töö kvaliteet ja tootlikus ei kannataks.<sup>201</sup> Kaugtöö töötajapoolsete eelistena on uuringus välja toodud tööga rahulolu ja produktiivuse üldist kasvu ning aja ja kulude kokkuhoiu. Samuti on töötajad leidnud, et kaugtöö tõttu on neil tulnud omandada uusi oskusi ja teadmisi, kuivõrd neil tuleb probleeme iseseisvalt lahendada.<sup>202</sup> Miinustena on eelkõige mainitud professionaalset ja sotsiaalset eraldatust, mis omakorda vähendab nii õppimis- kui karjäärivõimalusi. Samuti on negatiivse asjaoluna mainitud eraelu ja tööelu vahelise piiri kadumist.<sup>203</sup>

Statistikaameti poolt 2015. aastal läbi viidud tööelu uuringust nähtub, et väljaspool kontoriruumi sooviks tööd teha 34% küsitletutest,<sup>204</sup> kuid realsuses võimaldab kaugtööd teha üksnes 18% organisatsioonidest.<sup>205</sup> Sotsiaalministeerium näeb kaugtöö tegemise kasvuks tulevikus suurt potentsiaali, sest üha suurenev tööjõupuudus sunnib tööandjaid pakkuma töötajatele paindlikemaid töötingimusi.<sup>206</sup> Suurenev vajadus aga tähendab seda, et ka tööõigus peab suutma ajaga sammu pidada ning õiguslikult tuleb tagada mõlema poole õiguste realiseerimine ka kaugtöö puhul.

Euroopa tasandil on vaatlusalune valdkond reguleeritud Euroopa Sotsiaalpartnerite 2002.

---

<sup>200</sup> K.Künnapas. Kaugtöö aktuaalseid probleeme. *Juridica* IV/2014 lk 279

<sup>201</sup> E. Kallaste, K. Jaakson (koost.) Eesti Rakendusuuringu Keskus Centar. Kaugtöö Eesti organisatsioonides. 2009, lk 5

<sup>202</sup> sama lk 11-13

<sup>203</sup> sama lk 14-17

<sup>204</sup> L. Kaldmäe (toim.) Eesti tööelu uuring 2015. Sotsiaalministeerium. Analüüsi ja statistika osakond. lk 12. Arvutivõrgus: [https://www.sm.ee/sites/default/files/content-editors/Ministeerium\\_kontaktid/Uuringu\\_ja\\_analuusid/eesti\\_tooelu\\_uuring\\_2015.pdf](https://www.sm.ee/sites/default/files/content-editors/Ministeerium_kontaktid/Uuringu_ja_analuusid/eesti_tooelu_uuring_2015.pdf) 29.03.2017

<sup>205</sup> sama lk 14

<sup>206</sup> L. Kaldmäe. Kui levinud on Eestis kaugtöö vormis töötamine? – Tööelu portaal. 29.03.2017. Arvutivõrgus: <http://www.tooelu.ee/et/uudised/uuringud-ja-analysid/1514/tooelu-uuring-kui-levinud-on-eestis-kaugtöö-vormis-tootamine> 29.03.2017

aasta kaugtööd käsitleva raamkokkuleppega, mille artikli 2 kohaselt on kaugtöö töö korraldamise ja/või -teostamise vorm, kus infotehnoloogia abil ja töölepingu või töösuhte kontekstis tehakse tööd väljaspool tööandja ruume, kuigi tööd oleks võimalik teha ka tööandja ruumides.<sup>207</sup>

Töölepinguseadus kaugtöö definitsiooni *expressis verbis* ei anna, sedastades üksnes, et olukorras, kus töötaja ja tööandja lepivad kokku, et töötaja teeb tööd, mida tavapäraselt tehakse tööandja ettevõttes, väljaspool töö tegemise kohta, sealhulgas töötaja elukohas (kaugtöö), tööandja kohustuse töötajat teavitada, et tööd tehakse kaugtööna.<sup>208</sup> Seega mõistetakse Eesti õiguses kaugtööna mistahes tööd, mida tehakse tööandja ja töötaja kokkuleppel väljaspool töö tegemise kohta (enamasti siis tööandja ruume). Muus osas igasugune õiguslik regulatsioon kaugtöötamise osas puudub.

Soome tööseaduses on üldsätetes välja toodud, et seadust kohaldatakse vaatamata sellele, kus on töötaja töökoht või kas ta kasutab tööandja töövahendeid.<sup>209</sup> Töötervishoidu ja -ohutust reguleeriv seadus aga toob konkreetselt välja, et seadust rakendatakse ka kaugtöö puhul, kuid töökeskkonna ohutuse tagamisel, riskianalüüsi koostamisel ja ohutu töökeskkonna loomisel võetakse arvesse, et tööandjal puudub voli eelnimetatud asjaolusid mõjutada ning pannakse töötervishoiu ja -ohutusnõuete järgmise risk töötajale.<sup>210</sup>

Töösuhte üheks peamiseks tunnuseks on töö tegemine tööandja kontrolli all ja juhtimisel.<sup>211</sup> Klassikalises võtmes eeldab töötamine igapäevast töötaja kohalolekut tööandja ruumides ning 40-tunnist töönädalat,<sup>212</sup> mis muudab tööandjapoolse kontrolli töö tegemise üle ja juhtimise võrdlemisi lihtsaks. Kuigi kaugtöö puhul tuleb tööandjal esmalt kaugtöö tegemise juhendid ja korrad välja töötada, muutub töö tegemise faktiline kontrollimine suhteliselt võimatuks, sest näiteks kodustöötava töötaja puhul vastandub tööandja kontrolliõigusele töötaja

---

<sup>207</sup> E. Käärats, M. Talur (koost.) Sotsiaalministeerium. Tööelu arengu osakond. Euroopa Liidu Sotsiaalpartnerite raamkokkulepe kaugtöö kohta. Kogumik. Tallinn: Ilo, 16.02.2002, lk 49 Arvutivõrgus:

[https://www.sm.ee/sites/default/files/content-editors/eesmargid\\_ja\\_tegevused/Too/Tookeskkond/el\\_sotsiaalpartnerite\\_raamkokkulepete\\_kogumik.pdf](https://www.sm.ee/sites/default/files/content-editors/eesmargid_ja_tegevused/Too/Tookeskkond/el_sotsiaalpartnerite_raamkokkulepete_kogumik.pdf)  
29.03.2017

<sup>208</sup> TLS § 6 lg 4

<sup>209</sup> *Työsopimuslaki* § 1

<sup>210</sup> *Työturvallisuuslaki* § 1 lg 5. Arvutivõrgus inglisekeelsena:

<http://www.finlex.fi/en/laki/kaannokset/2002/en20020738.pdf> 30.03.2017

<sup>211</sup> TLS § 1 lg 1

<sup>212</sup> TLS §§ 20 ja 43 lg 1

põhiõiguslik kodupuutumatus, mille piiramine on võimalik vaid seaduse alusel, silmas pidades ka proportsionaalsuse põhimõtet.<sup>213</sup>

Enesestmõistetavalt puudub tööandjal voli töötaja kodus omaalgatuslike kontrollvisiitide tegemiseks. Siiski võib teatud juhtudel töökohustuste täitmisel tekkivate probleemide ennetamiseks tekkida vajadus töötaja töökohta kontrollimiseks. Töötervishoiu ja tööohutuse seaduse §§ 4 lg 2 ja 12 lg 1 kohustavad tööandjat looma töökoht selliselt, et on võimalik vältida tööõnnetusi ja tervisekahjustusi ning säilitada töötaja töövõime ja heaolu igas tööga seotud olukorras. Seejuures mõistetakse TTOS § 4 lg 1 tähenduses töökohana muuhulgas ka kohta, kus töötaja töötab tööandja loal või korraldusel.

Magistritöö autori hinnangul saab siinkohal kaugtöötamist arvesse võttes töökohana käsitleda ka töötaja kodu. Seega on põhimõtteliselt tööandja kohustuseks tagada töötaja ohutu ja töötervishoiu reeglitele vastav töökoht ka töötaja enda kodus. Antud käsitlust toetab ka kaugtöö raamkokkulepe, mille artikli 8 kohaselt on tööandjal, töötajate esindajal ja/või vastavatel võimudel õigus kontrollida ka kaugtöö tegemise kohas kas tööandja poolt kehtestatud töötervishoiu ja -ohutuse reegleid järgitakse kindlaksmääratud korras ja ulatuses. Kodus töötamise puhul on juurdepääs töökohale võimalik üksnes etteteatamise ja töötaja sellekohase nõusolekuga. Samuti on raamkokkuleppega antud töötajal põhimõtteline õigus ise taotleda vastava inspeksiooni läbiviimist.<sup>214</sup>

Lisaks eeltoodule on ka kaugtöö puhul tööandja peamiseks huviks ärisaladuse hoidmine ja konkurentsi piiramine. Ehkki tegemist on töölepinguseadusest tulenevate töötaja kohustustega, on tööandjal kaugtöötajat ning tema tegevusi aga oluliselt keerulisem kontrollida, seda eriti olukorras, kus töötaja teeb tööd läbi isikliku seadme, mitte tööandjale kuuluva arvuti vahendusel. Eeltoodust tulenevalt on kaugtöötamise puhul kaitstud küll töötajate eraelu, kuid tööandjate majanduslikud huvid on seetõttu rohkem ohustatud.

Vaatamata sellele, et kaugtöötamise vorm kui selline on muutumas üha populaarsemaks, puuduvad selle rakendamiseks konkreetsed nõuded, mis hõlbustaksid ka võimalike probleemide ja vaidluste lahendamist. Magistritöö autori soovitusel tuleks kaugtöö puhul

---

<sup>213</sup> O. Kask, H. Sepp. Põhiseaduse kommentaar §-le 33 p. 22

<sup>214</sup> Kaugtöö raamkokkulepe lk 53

töölepingus fikseerida kaugtöötamise tingimused (näiteks töö- ja kommunikatsioonivahendite soetamine ja kasutamine; olenevalt töö iseloomust ka näiteks kaugtööl tehtava töö maht nädalas või kalendrikuus jms), samuti ka tööandja ja/või kolmandate isikute juurdepääsu õiguse tingimused töökohale (näiteks etteteatamise tähtaeg ja kord).

### 3.7. Rahvusvahelised töösuhted

#### 3.7.1 Euroopa ja USA andmekaitsealane koostöö

Eesti on maailmas tuntud oma tehnoloogialembuse ja idufirmasid soosiva majanduskeskkonna poolest. Näiteks kirjutas mainekas väljaanne *The Wall Street Journal*, et just siin asutatakse kõige rohkem idufirmasid Euroopas<sup>215</sup> ning ajakirjas *The Bloomberg View* on tunnustatud eestlasi ka selle eest, et teatakse eduka *start-up*'i valemit.<sup>216</sup> Ühtlasi viidatakse aga ka sellele, et Eesti jääb mingil hetkel ettevõttele kitsaks – investorid soovivad tegutseda (majandus)keskkonnas, mida nad paremini tunnevad ning ka tõeliselt väärtuslikud kliendid asuvad Eestist väljaspool.<sup>217</sup> Nii ongi tuntumatel iduettevõtetel nagu Skype, TransferWise, PlayTech, Testlio jne (pea)kontorid lisaks Tallinnale ka mujal maailma paigus – San Franciscos, Londonis, New Yorgis. See tõstatab omakorda küsimuse, millise riigi õigust ja andmekaitse reegleid sellisel juhul töösuhtele kohaldada?

Probleemid Euroopa Liidu liikmesriikide ja USA vahelises isikuandmete vahetamises tõusetusid esmakordselt 1990ndate lõpus kui Euroopa Liidu esindajad avaldasid, et kuigi USA on *de jure* OECD isikuandmete kaitse põhimõtted ja suunised omaks võtnud, siis tegelikkuses ei ole isikute põhiõigused selles valdkonnas sugugi tagatud.<sup>218</sup> Selle valguses sündis 26.07.2000. Euroopa ja USA vaheline isikuandmete kaitse alane koostöölepe „*Safe Harbour*“,<sup>219</sup> mis toimus suhteliselt kenasti terve dekaadi, kuid tulenevalt USA

---

<sup>215</sup> B. Rooney. *The Many Reasons Estonia is a Tech Start-up Nation*. - *The Wall Street Journal*. 14.06.2012

<sup>216</sup> L. Bershidsky. *Estonian's Overhyped Silicon Valley*. - *The Bloomberg View*. 05.03.2015.

<sup>217</sup> sama

<sup>218</sup> *Article 29 Data Protection Working Party. Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"* 16.05.2000.

<sup>219</sup> Euroopa Komisjoni otsus 26. juuli 2000, 2000/520/EC, vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium. ELT 25.08.2000. L 251

sisejulgeolekupoliitika eripäradest ei suudetud siiski tagada isikuandmete kaitset samal tasemel, kui Euroopas.

Nii juhtiski 29.04.2010 Saksamaa andmekaitse ja teabevabaduse volinik tähelepanu sellele, et Euroopa ettevõtted, kes ekspordivad isikuandmeid USA-sse peaksid vähemalt ise veenduma selles, et *Safe Harbor*'i nõudeid realselt vastuvõtja (USA) poolt ka järgitakse.<sup>220</sup> Sellele järgnes mitme aasta pikkune riikidevaheline dialoog selles, et koostööd tuleb jätkata ning pidevalt tehakse selles suunas pingutusi,<sup>221</sup> kuid reaalselt tulemust ei suudetud siiski saavutada ning Euroopa Kohtu 2015. otsusega tunnistati *Safe Harbor* sisuliselt läbikukkunuks.<sup>222</sup>

Diskussioon ning lahenduste otsimine siiski jätkus ning 02.02.2016 tutvustas Euroopa Komisjon uut transatlantilist andmetevahetuse raamkokkulepet – „*Privacy Shield*“,<sup>223</sup> mis jõustus 12.07.2016 ning mille olulisimaks täienduseks võrreldes oma eelkäijaga on asjaolu, et eurooplastele anti õigus USA kohtu poole pöörduda, kui on alust arvata, et ameeriklased ei järgi Euroopa Liidus kehtivaid andmekaitse nõudeid.<sup>224</sup> Samuti sedastati selged ja ranged kohustused andmeid töötlevatele äriühingutele ning nähti ette kindlad alused ja kaitsemeetmed seoses USA julgeolekuasutuste ligipääsuga andmetele.<sup>225</sup>

Vaatamata sellele, et „privaatsuskilp“ on olnud aktiveeritud käesoleva töö esitamise ajal ligi aasta, on selle vastupidavus juba proovile pandud. Nimelt esitas 16.09.2016 privaatsuse

---

<sup>220</sup> Voliniku otsus allalaetav *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen* koduleheküljel:

[https://www.lidi.nrw.de/mainmenu\\_Service/submenu\\_Entschliessungsarchiv/Inhalt/Beschluesse\\_Duesseldorfer\\_Kreis/Inhalt/2010/Pruefung\\_der\\_Selbst-Zertifizierung\\_des\\_Datenimporteurers/Beschluss\\_28\\_29\\_04\\_10neu.pdf](https://www.lidi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteurers/Beschluss_28_29_04_10neu.pdf) 22.02.2017

<sup>221</sup> Nt. 19.03.2013 Euroopa Komisjoni asepresidendi ja USA asjakohase ametniku ühisavaldus. Kättesaadav: <http://2010-2014.commerce.gov/news/press-releases/2012/03/19/us-eu-joint-statement-privacy-eu-commission-vice-president-viviane-re.html> 22.02.2017; 19.07.2013 Euroopa Komisjoni asepresidendi avaldus Justiitsnõukogu kogunemisel Vilniuses. Kättesaadav: [http://europa.eu/rapid/press-release\\_MEMO-13-710\\_en.htm](http://europa.eu/rapid/press-release_MEMO-13-710_en.htm) 22.02.2017 ; 28.01.2014 Euroopa Komisjoni pressiteade andmekaitse tähtsusest Euroopas. Kättesaadav: [http://europa.eu/rapid/press-release\\_SPEECH-14-62\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm) 22.02.2017; D. Sarmadi. Ansip threatens to suspend Safe Harbour data agreement with US.07.10.2014. Kättesaadav: <http://www.euractiv.com/section/innovation-industry/news/ansip-threatens-to-suspend-safe-harbour-data-agreement-with-us/> 22.02.2017

<sup>222</sup> Euroopa Kohtu 06.10.2015 otsus C-362/14. *Schrems vs Digital Rights Ireland*.

<sup>223</sup> Euroopa Komisjoni 02.02.2016 pressiteade. Kättesaadav: [http://europa.eu/rapid/press-release\\_IP-16-216\\_en.htm](http://europa.eu/rapid/press-release_IP-16-216_en.htm) 22.02.2017

<sup>224</sup> H. Lõugas. Privaatsuskilp hakkas tööle: eurooplasted saavad andmekaitseks nüüd USA kohtusse pöörduda. 07.12.2016. Geenius digiuudiste portaal.

<sup>225</sup> Euroopa Komisjoni 12.07.2016 pressiteade *Privacy Shield* jõustumise kohta. Kättesaadav: [http://europa.eu/rapid/press-release\\_IP-16-2461\\_et.htm](http://europa.eu/rapid/press-release_IP-16-2461_et.htm) 22.02.2017

kaitse tagamisele suunatud organisatsioon *Digital Rights Ireland* Euroopa Kohtusse hagi, millega taotleb, et kohus tuvastaks oma 12.07.2016 a rakendusotsuses EL 2016/1250 tehtud hindamisvea ELi-USA andmekaitseraamistiku *Privacy Shield* isikuandmete kaitse piisavuse kohta vastavalt Euroopa Parlamendi ja nõukogu direktiivile 65/46 EÜ (andmekaitse direktiiv) põhjusel, et kohus leidis oma otsuses, et isikuandmete kaitse tase on USA-s piisav ja vastab andmekaitse direktiivi nõuetele.<sup>226</sup> 22.11.2017 Euroopa Kohtu määrusega keelduti hagi menetlemast õigustatud huvi puudumise tõttu.<sup>227</sup>

Privaatsuskilbi“ tõeline proovikivi saab aga ilmselt alguse 25.05.2018, kui liikmesriides jõustub andmekaitsemäärus, millega võrreldes direktiiviga nõudeid veelgi karmistatakse.<sup>228</sup> Asjaolude selginemiseni tuleb lähtuda põhimõttest, et eurooplaste andmeid tuleb ka USA-s töödelda meil kehtivate nõuete ja reeglite kohaselt ehk siis kuni 25.05.2018 tuleb Eesti ettevõtetel aluseks võtta IKSi asjaomased sätted ning hiljem GDPR koostoimes uue IKSi

### 3.7.2. Väärkäitumisest teatamine

Väärkäitumisest teatamine on omamoodi seotud Euroopa-USA andmekaitsealase koostööga, kuid seda pigem vastupidises mõttes. USA kongress võttis 30.07.2002 vastu *Sarbanes-Oxley* seaduse (edaspidi SOX), mille kohaselt peavad USA-s registreeritud ettevõtted ja nende Euroopas asuvad haruettevõtted ning ka USA (New York'i või Nasdaq'i) aktsiaturul noteeritud välisriikide ettevõtted esiteks looma efektiivse kontrollsüsteemi oma juhtimise ja raamatupidamise üle ning samuti ka konfidentsiaalse ja anonüümse mehhanismi, millega töötajad saaksid teatada raamatupidamise või auditeerimisega seotud kahtlustest.<sup>229</sup> Seejuures kohustuvad eelmainitud ettevõtted ka igal aastal kinnitama, et nad täidavad ettenähtud eeskirju, sh ka väärkäitumisest teatamisega seonduvaid nõudeid.<sup>230</sup>

---

<sup>226</sup> *Digital Rights Ireland* 16.09.2016 esitatud hagi. Kohtuasi T-670/16 *Digital Rights Ireland v Commission*

<sup>227</sup> 22.11.2017 *Order of the General Court (Second Chamber) Case T-670/16 Digital Rights Ireland v Commission*

<sup>228</sup> Nt sedastab GDPR art 3 lg 1, et määruse sätted on kohustuslikud liidus asuvalle andmetöötajale (sh rahvusvaheliste ettevõtete filiaalid, tütarettevõtted, esindused jms), sõltumata sellest, kus andmeid tegelikult töödeldakse.

<sup>229</sup> *107th Congress of United States of America. 30.07.2002 Sarbanes-Oxley Act of 2002*. Kättesaadav: <https://www.sec.gov/about/laws/soa2002.pdf> 05.03.2017

<sup>230</sup> AKI juhendmaterjal lk 84

Sisuliselt paneb SOX ettevõtetele kohustuse sisse seada süsteem, mille kaudu saaks üks töötaja anonüümselt teada anda teise töötaja väärkäitumisest. Euroopa Andmekaitseasutuste töögrupp on välja toonud asjaolu, et kuna ettevõtete teatamismehhanismid ei ole üldjuhul avalikud, ei ole teada, kas need on kooskõlas Euroopa andmekaitsealusega ega ka seda mismoodi lahendatakse vastuolud. Seega võib tekkida olukord, kus üks ettevõtte võib saada karistatud Euroopas selle eest, et andmekaitsealuseid on rikutud ja USA-s selle eest, et SOX eeskirju ei ole täidetud.<sup>231</sup>

Et SOX annab ettevõtetele suhteliselt vabad käed teatamismehhanismide loomiseks on Euroopa Andmekaitseasutuste töögrupp oma arvamuses andnud üldise hinnangu mehhanismide seaduspärasusele, leides, et isikuandmete töötlemine oleks andmekaitsealusega kooskõlas kahel juhul: a) mehhanismi loomine on vajalik selleks, et täita seadusjärgset kohustust (artikli 7 lg 1c); b) mehhanismi loomine on vajalik selleks, et ellu viia vastutava töötaja või andmeid saava kolmanda isiku õigustatud huvisid (art 7 lg 1f).<sup>232</sup>

Kuivõrd SOX ei ole kehtestatud ühegi liikmesriigi õiguse alusel, ei saa töögrupi hinnangul mehhanismide puhul tugineda art 7 lg 1 punktile c.<sup>233</sup> Andmekaitse Inspeksioon on siiski aga leidnud, et Eesti õiguses võib selliseks juriidiliseks kohustuseks pidada Krediidiasutuste seaduses sisalduvat kohustust kehtestada sise-eeskirjad ja protseduurireeglid töötajate huvide konfliktide vältimiseks.<sup>234</sup>

Teisel juhul võib andmekaitse töögrupi hinnangul teatamismehhanismide loomine olla vajalik selleks, et ellu viia vastutava töötaja või andmeid saava kolmanda isiku õigustatud huvisid tingimusel, et need ei kaalu üles andmesubjekti põhiõiguste ja -vabadustega seotud huve.<sup>235</sup>

Nii Euroopa Liit kui OECD peavad oluliseks äriühingute juhtimise läbipaistvust, et tagada ühingute tõhus toimimine ning rõhutavad, et asjakohaste meetmete ja süsteemide loomine, mis võimaldavad rikkumistest ja väärkasutustest teada anda, peaks olema iga organisatsiooni

---

<sup>231</sup> Article 29 Data Protection Working Party. *Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime*. 01.02.2006, lk 5

<sup>232</sup> sama lk 7

<sup>233</sup> sama lk 8

<sup>234</sup> AKI juhendmaterjal lk 85

<sup>235</sup> Vnr 231, lk 8

huvides.<sup>236</sup>

Väärrib rõhutamist, et lisaks SOX-ist tulenevale kohustusele, leiab ohust või rikkumisest teavitamise kohustusi erineval kujul ka Eesti siseriiklikest õigusaktidest, näiteks korruptsiooni vastase seaduse § 6, karistusseadustiku<sup>237</sup> §-d 306–307, keskkonnastutuse seadus<sup>238</sup> § 9 ning ka töötervishoiu ja tööohutuse seadus § 14, küll aga takistab teatamiskohustuse täitmist asjaolu, et rikkumisest teataja kaitse tööandja või kaastöötajate ees on nõrk või isegi puudlik<sup>239</sup> ning käsitlemise negatiivne kuvand.<sup>240</sup> Seega tasub teemat Eesti kontekstis lähemalt uurida.

TLS § 15 lg 2 p 8 kohustab töötajat teavitama tööandjat viimase soovil kõigist töösuhete seonduvatest olulistest asjaoludest, mille vastu tööandjal on õigustatud huvi, kuid AKI hinnangul on äärmisel kaheldav, kas „vilepuhumine“ võiks samuti selle konteksti alla mahtuda.<sup>241</sup>

Vastupidiselt AKI seisukohale, on praktikud leidnud, et kui ühele töötajale saab teatavaks asjaolu, et teine töötaja paneb selgelt toime lepingulise kohustuse rikkumise (näiteks omastab tööandja vara), siis on tegemist olulise asjaoluga, mille suhtes on tööandjal õigustatud huvi. Ühendkuningriigi kohtupraktikale tuginedes, on T. Tiits välja toonud ka avaliku huvi kriteeriumi, mille kohaselt on informatsiooni avalikustamine õiguspärane siis, kui see on tehtud „rikkumisest teavitajast töötaja mõistlike veendumuste kohaselt avalikes huvides.“<sup>242</sup> Erinevate majandusalaste süütegude puhul on selline avalik huvi ilmne. Seega on AKI seisukoht ekslik selles, et TLS § 15 lg 2 p-s 8 sedastatud kohustusena tuleb käsitleda üksnes töötaja enda andmeid.<sup>243</sup>

---

<sup>236</sup> Vnr 231 lk 9

<sup>237</sup> Karistusseadustik – RT I 30.12.2017, 29

<sup>238</sup> Keskkonnastutuse seadus – RT I 10.11.2016, 8

<sup>239</sup> T. Tiits. Rikkumisest teavitamisega seonduvaid probleeme Eestis. *Juridica* VI/2014, lk 443

<sup>240</sup> Sama, lk 446

<sup>241</sup> AKI juhendmaterjal lk 85

<sup>242</sup> Tiits, lk 452

<sup>243</sup> M. Liis. Andmekaitse inspeksiooni jäik seisukoht raskendab USA börsireeglite täitmist. Advokaadibüroo Eversheds Ots & Co uudisteblogi. 29.03.2016. Kättesaadav: <http://www.eversheds.ee/global/en/where/cee/estonia/-ee/overview/news/shownews.page?News=en/estonia/ee/Andmekaitse-inspeksiooni-jaik-seisukoht-raskendab-USA> 10.03.2017



GDPR-is on isikuandmete töötlemise seaduslikkuse alused välja toodud artiklis 6, kus mõnevõrra on punktide b ja c sõnastust muudetud, kuid nende põhiolemus jääb samaks. Isikuandmete töötlemine on seaduslik, kui see on vajalik vastutava töötleja juriidilise kohustuse täitmiseks (art 6 punkt c) või kui see 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 isikuandmeid kaitsta (art 6 punkt f).

Magistritöö autorile teadaolevalt on asjakohased meetmed rikkumisest teataja õiguste kaitseks tarvidusele võetud Suurbritannias,<sup>244</sup> Iirimaal<sup>245</sup> ja Hollandis<sup>246</sup> ning juba 2010. aastal kutsus Euroopa Nõukogu Parlamentaarne Assamblee oma resolutsioonis nr 1729 liikmesriike üle vaatama oma rikkumisest teavitamise alased reeglid või nende puudumisel looma normid, mis kaitseksid isikute õigusi nii era- kui avalikus sektoris.<sup>247</sup> Eesti puhul on AKI viidanud, et sellise meetmena võiks käsitleda Krediidiasutuste seaduses sisalduvat kohustust kehtestada sise-eeskirjad ja protseduurireedid töötajate huvide konfliktide vältimiseks.<sup>248</sup> Siiski ei ole see kohaldatav iga ettevõtte puhul, mistõttu on magistritöö autori hinnangul teamismehhanismide loomisel mõttekam juriidilise kohustuse asemel tugineda GDPR art 6 lg 1 p-le f ehk vastutava töötleja õigustatud huvile.

Tööandja, kui vastutava töötleja õigustatud huvi on hinnanguline kriteerium, mille puhul ei saa magistritöö autori hinnangul lähtuda mingitest üldistest alustest ega standarditest. Eelkõige on tööandja õigustatud huvi seotud sellega, et tema ettevõtte oleks hästitoimiv ja kasumlik ning selle tagamiseks on ettevõtetel võimalus rakendada väga erinevaid praktikaid, millede teostamine on ühelt poolt lubatud ettevõtlusvabadusega, kuid teisalt piiratud teiste asjakohaste õigusaktidega, nt maksuseadused, töölepinguseadus jms.

Kehtiva töölepinguseaduse kohaselt on tööandjal õigus nõuda töötajalt informatsiooni selliste

---

<sup>244</sup> *Public Intrests Disclosure Act* 1998. Chapter 23. Kättesaadav:

<http://www.legislation.gov.uk/ukpga/1998/23/introduction/enacted> 10.02.2017

<sup>245</sup> D. Breadun. *Whistleblower Bill to Cover Public and Private Sectors. The Irish Times.* 30.01.2012.

Kättesaadav: <http://www.irishtimes.com/news/whistleblower-bill-to-cover-public-and-private-sectors-1.453932> 10.02.2017

<sup>246</sup> Autori märkus: sisse on seatud spetsiaalsed nõustamiskeskused, mis pakuvad „vilepuhujatele“ igakülget juriidilist tuge. Nt. *Adviespunt Klokkenuiders* <https://huisvoorklokkenuiders.nl/> 10.02.2017

<sup>247</sup> Viidatud T. Tiits kaudu (vnr 5)

<sup>248</sup> AKI juhend lk 85

töösuhtega seonduvate asjaolude kohta, mille vastu võiks tööandjal olla õigustatud huvi.<sup>249</sup> Töölepinguseaduse seletuskiri märgib, et eelviidatud teavitamiskohustuse sisuks on tagada töösuhte läbipaistvus ning pooltevaheline usaldus.<sup>250</sup> Töötaja kohustub oma töökohustusi täitma lojaalselt, oma teadmiste ja oskuste kohaselt tööandja kasu silmas pidades ning töö iseloomust tuleneva vajaliku hoolsusega.<sup>251</sup> Töölepinguseaduse seletuskiri märgib, et tööandja õigustatud huvi puhul võetakse arvesse ka Võlaõigusseaduse §-s 7 sätestatud mõistlikkuse põhimõtet, mille alusel ei saa tööandja eeldada, et töötaja annaks teada asjaoludest, millest teatamist ei eeldaks samas olukorras heas usus tegutsev isik, kuna ta ei pea teatud asjaolu teatamist vajalikuks ega mõistlikuks.<sup>252</sup>

Eeltoodule tuginedes on käesoleva magistritöö autor seisukohal, et tööandjal on õigus tekitada oma töötajatele kohustus tööandjat teavitada kõigist töösuhte (sh üldise töökeskkonnaga) seonduvatest asjaoludest, mille suhtes võiks tööandjal mõistlikult võttes olla õigustatud huvi ning mille alusel saab tööandja teha vastavaid ümberkorraldusi. Seega võib järeldada, et edaspidi muutub „pealekaebamine“ põhimõtteliselt õiguspäraseks.

Peatüki vahekokkuvõtteks saab välja tuua järgmised aspektid:

- tööandjale on antud kontrolliõigus, kuid selle teostamine peab toimuma viisil, mis ei riivaks liigselt töötaja privaatsust;
- nii nagu töötaja ei jäta oma eraelu tööle tulles ukse taha, kohustub ta ka töösuhte väliselt kandma organisatsiooni väärtuseid ja hoidma tööandja ärisaladust;
- andmekaitser reformi valguses on tööandjatel mõistlik luua või üle vaadata ning vajadusel täiendada oma siseregulatsioonid nii töötaja kontrollmiseks, oma kohustuste täitmiseks kui ka töötajate õiguste tagamiseks.

---

<sup>249</sup> TLS § 15 lg 2 p 8

<sup>250</sup> TLS seletuskiri lk 24

<sup>251</sup> TLS § 16 lg 1

<sup>252</sup> TLS seletuskiri lk 24

## KOKKUVÕTE

Info- ja kommunikatsioonitehnoloogia areng ning sotsiaalmajanduslikud muutused ühiskonnas on endaga kaasa toonud ka töötamise ja töökeskkonna teisenemise, mis ühest küljest küll võimaldab töötajatele suuremat iseseisvust ning tagab laialdaselt nende eraelu kaitse, kuid nõrgestab tööandja kontrolliõigust, mistõttu on tööandjal üha raskem tagada oma ärisaladuse kaitset ja piirata konkurentsi.

Käimasoleva andmekaitsereformiga saavad töötajad veelgi laiaulatuslikuma kaitse oma andmete üle, samas kui tööandjate informatsiooni saamise õigus ning majanduslikud huvid jäävad pigem tahaplaanile. Ometigi on reformiga tööandjate kui vastutavate andmetöötlejate vastutust märkimisväärsete trahvidega laiendatud. Eeltoodust tulenevalt on käesoleval ajal eriti oluline analüüsida poolte huvide vastandumist ning leida nende vahel tasakaal töösuhte mõistlikuks toimimiseks.

Käesolev töö põhineb hüpoteesil, et teisenenud töökeskkonnas ei ole tööandjal võimalik oma GDPR-st tulenevat vastutava töötaja vastutust sisustada, kuivõrd see takistab tema ettevõtlusvabaduse raames tagatud kontrolliõiguse realiseerimist.

Hüpoteesi kontrollimiseks on töö jagatud kolme peatükki, millest esimene avab põhimõisted ning sedastab töötaja ja tööandja vastanduvad õigused, milleks kõige laiemas tähenduses on töötaja eraelu ja tööandja ettevõtlusvabadus, mis hõlmab ka tööandja kontrolliõigust.

Teises peatükis selgitati isikuandmete töötlemise õiguslikke aluseid värbamisprotsessis, ehk ajal mil pooled ei ole veel omavahel lepingulises suhtes, mistõttu saab andmete töötlemise õiguslikuks aluseks reeglina olla kandidaadi nõusolek. Nagu selgus töös viidatud K. Visamaa bakalaureusetöö käigus läbi viidud uuringust, kasutavad paljud tööandjad sotsiaalmeediat kandidaadi kohta taustauuringu tegemiseks või tööintervjuuks ettevalmistumiseks. Arvestades sotsiaalmeedia laialdast kasutust, pidas 2017 aasta suvel Euroopa Andmekaitseasutuste töögrupp vajalikuks avaldada tööandjatele suunised, milles rõhutatakse, et isegi kui kandidaadil on avalikult kättesaadav profiil mõnes sotsiaalvõrgustikus, siis ei tohiks tööandja neid värbamisprotsessis kasutada. Täielikult taunib töögrupp nõ sõbrakutsete saatmist eesmärgil veelgi rohkema informatsiooni teadasaamiseks. Juhul, kui tööandja on

siiski avalikult kättesaadavat infot kandidaadi kohta kogunud, kohustub ta sellest kandidaati teavitama. Vastav kohustus on sedastatud ka GDPR-i art-s 14.

Nagu töös selgitatud hõlmab tööandja ettevõtlusvabadus mh ka otsustusõigust selle üle, kellega töösuhet sõlmida. Arvestades tööandja eesmärki, milleks on ettevõttevõtte kasumlikkus, on tööandja põhiliseks huviks leida kvalifitseeritud töötaja, kes jagaks ettevõtte väärtuseid ning sobiks ka olemasoleva kollektiiviga. Visamaa bakalaureusetööst selgus huvitava aspektina ka see, et isegi kui tööandjal endal ei ole sotsiaalmeedias aktiivselt figureeriva töötaja vastu midagi, siis võiks selline seos ebamugavust tekitada mõnes ettevõtte konservatiivsemas kliendis. Oma huvide kindlustamiseks vajab tööandja seega kandidaadi kohta informatsiooni sageli isegi veel enne vestlusele kutsumise otsustamist. Ehkki informatsiooni saamise õigus kui selline on põhiseadusega tagatud, oleks GDPR-i kontekstis tegemist lubamatu andmetöötlusega, mida välistaks kandidaadi teavitamine tema kohta kogutud andmetest. See aga tundub olukorras, kus kandidaat on nangunii oma andmeid ja eraelu internetis avalikustanud, mõnevõrra kummastav ja tööandjale kahtlemata ka koormav, mistõttu on selles küsimuses tasakaal andmesubjekti õiguste ja vastutava töötleja õiguste ja kohustuste vahel paigast ära.

Kolmandas peatükis käsitleti IKT arengute ja sotsiaalmajanduslike muutuste tõttu teisenenud töökeskkonda, sh internetisuhtluse osas kontrolli teostamist. Kui töötaja kontrollimine on iseenesest õiguspärane tegevus, siis tuleb tööandjal eelnevalt paika panna vastavad sisekorralduslikud reeglid, mis hõlmaksid nii jälgimise/kontrollimise võimalikkust, kui selle ulatust; neid töötajale tutvustada ning võtta tarvitusele meetmed, mis riivaksid töötaja eraelu minimaalselt. G. Kempeli ja H. Urbeli magistritöödest ilmnes, et hoopis tõsisemaid probleeme, kui tööalane kommunikatsioon, võib tööandjale põhjustada töötajapoolne sotsiaalmeedia väärkasutus töövälisel ajal. Magistritöös oli välja toodud hulk juhtumeid nii era- kui avalikõiguslikes töösuhetes, kus töötaja ebakohased postitused või internetisuhtlus oli ettevõttele tekitanud mainekahju. Käesoleva magistritöö autor jagab seisukohta, et nii nagu töötajad ei jäta oma eraelu tööle tulles ukse taha, on nad seotud tööandjaga ka väljaspool tööaega ning kohustuvad ka siis jagama tööandjaga samu väärtuseid, hoidma ärisaladust ning kinni pidama konkurentsipiirangust. Objektiivsetel põhjustel ei ole aga tööandjal võimalik töötaja erakanalites aset leidva kommunikatsiooni üle kontrolli teostada.

Sisuliselt puudub tööandjal kontrolliõigus ka kaugtöö puhul ja seda ka töötervishoiunõuete osas. Näiteks kohustab TTOS tööandjat tagama ohutu töökeskkonna, kuid see ei ole võimalik olukorras, kus töö tegemise kohaks on töötaja kodu. Samas lasub tööandjal siiski vastutus tööõnnetuste või kutsehaiguste puhul. Teisalt puudub kontrollimise õigus ja võimalus ka ärisalduse hoimise ja konkurentsipiirangu osas, seda eriti siis, kui töötaja teeb tööd isikliku arvuti vahendusel. Seega on kaugtöö puhul igakülgset kaitstud küll töötaja eraelu, kuid tööandja huvid jäävad tahaplaanile.

Eeltoodust tulenevalt on hüpotees vähemalt osaliselt leidnud kinnitust. GDPR kohustab tööandjat kui vastutavat andmetöötlejat järgima kõiki määrusest tulenevaid isikuandmete töötlemise põhimõtteid ning kasutusele võtma mitmesuguseid korralduslikke, füüsilisi ja infotehnoloogilisi meetmeid isikuandmete kaitseks, kuid selle kohustuse täitmise käigus saavad kahjustada või jäävad täielikult tähelepanuta tööandja enda huvid. Andmekaitse nõuete rikkumisel näeb aga uus IKS vastutavale andmetöötlejale ette märkimisväärsed trahvid, seega on tööandja ettevõtlusega tagatud kontrolliõiguse rakendamine raskendatud või täiesti võimatu.

Käesoleva magistr töö eesmärk oli analüüsida kaasaegses töösuhtes ette tulevaid probleeme ning luua terviklik käsitus mõlema poole õigustest ja kohustustest. Töö praktiliseks väärtuseks on läbi käsitatud aktuaalprobleemide ja materiaalõiguse selgunud põhimõtted, mille alusel on ettevõtetel võimalik oma organisatsioonisiseseid toimimisjuhendeid luua või uuendada ning töötajaid koolitada.

1. Kandidaadi andmete töötlemine värbamisel saab toimuda üksnes andmesubjekti nõusoleku alusel (GDPR art 4 lg 2) või vastava juriidilise kohustuse olemasolu korral ka art 6 lg 1c alusel, mispuhul tuleb andmesubjekti töötlemisest teavitada (art 14);
2. Kandidaadi andmete kogumisel tuleb tööandjal leida tasakaal töösuhteks vajaliku õigustatud huvi ja andmete minimaalsuse põhimõtte (GDPR art 5 lg 1c) vahel.
3. Tööandja on kohustatud kandideerimismaterjali osas kehtestama säilitamise tähtajad (GDPR art 5 ja uus IKS § 16).
4. Töötaja isikuandmete kogumisel tuleb lähtuda tööandja õigustatud huvist, kogudes siiski üksnes sellist informatsiooni, mis on töösuhte tõrgeteta toimimiseks mõistlikult vajalik.
5. Töötaja isikuandmete avaldamiseks ettevõtte või asutuse koduleheküljel,

sotsiaalmeedias või mõnes muus kanalis on tööandjal mõistlik võtta töötaja kirjalik nõusolek siis, kui avaldatakse rohkem infot, kui pelgalt tööalane e-post ja kontakttelefon. Avalikustamisel tasub tööandjal siiski hinnata, kas see on töösuhte kontekstis vajalik ning kaalub üle töötaja eraelu kaitse.

6. Kontrollimehhanismide loomisel seada esmalt kontrollimise eesmärk ning panna paika selle ulatus; luua nendele vastavad siseregulatsioonid ning teha need töötajatele teatavaks; tagada töötajatele kaitsemeetmed kontrollist teavitamise puhuks (näiteks teavituskiri e-postkasti avamise kohta). Kontrollimehhanismide loomisel arvestada ka kaugtöötajatega.
7. Vajadusel luua oma ettevõttes ka sotsiaalmeedia kohase kasutamise juhised.
8. Kehtestada ettevõttes tähtjad töödokumentide säilitamisele ja hävitamisele.
9. Biomeetria kasutamisel eelistada seadmeid, mis loovad biomeetria abil üksnes ligipääsuks vajaliku koodi, kuid biomeetrilisi andmeid kuidagi ei säilitata, nt töötaja valduses olev sõrmejäljelugejaga telefon.
10. Töötaja eriliigiliste isikuandmete (tervisandmete) töötlemine on lubatud, kui see on rangelt vajalik ning üksnes siis kui töötlemise lubatavus on sätestatud õigusaktis või kui see on vajalik andmesubjekti või teise füüsilise isiku eluliste huvide kaitseks või töödeldakse selliseid isikuandmeid, mida andmesubjekt on ilmselgelt avaldanud (uus IKS § 19). Vajadusel tuleb tööandjal oma ettevõttes kehtestada siseregulatsioonid selliste andmete kogumise ja säilitamise osas.
11. Euroopa Liidu liikmesriigi kodanikust töötaja andmetele rakendub ka liiduvälisel töötamisel GDPR.
12. Vajadusel luua oma ettevõttes mehhanismid väärkäitumisest teatamise puhuks.

## BALANCING THE RIGHTS OF THE PARTIES IN THE CONTEXT OF MODERN EMPLOYMENT AND GENERAL DATA PROTECTION REGULATION. Abstract

Due to one party's economic interests colliding with other party's fundamental rights, employment relations are always complicated. According to the core principles of contract law the parties are equal, but in practice employment is more considered as sub ordinance, due to the employer's right to control the employee and the performance of his/her obligations.

As some form of working applies to a large part of population and people spend significant amount of their time at work, the European Data Protection Working Party has noted that employees do not abandon their right to privacy and data protection every morning at the doors of the workplace. They do have a legitimate expectation of a certain degree of privacy in the workplace as they develop a significant part of their relationships with other human beings within the workplace. Approach is based on the decision of case Niemietz vs Germany (1992) of the European Court of Human Rights, which explained that "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world.

As a result of the rapid developments of information and communication technology (ICT) and general socioeconomic matters in society, the form of working as well as the entire environment of working has changed. For example, next to the classic nine-to-five office work, performing duties is also possible on the basis of a flexible work schedule and telecommuting, which means that an employee is significantly more independent in his/her operations. On the one hand, such an increase of the independency supports the principle of equality of parties, but, at the same time it complicates practising the employer's right to control and monitor the employee, which may compromise the economic interests of the employer.

Regardless of the nature of the work or the place where it is performed, processing the employee's personal data is inevitable in the employment relationship due to the legitimate interest of the employer and in the performance of its statutory obligations. The Employment

Contracts Act imposes an obligation on the employer to respect and protect the employee's fundamental rights, including personal data, to which the current Personal Data Protection Act requires the employer, as the controller, to introduce different organisational, physical and information security measures. The ongoing reformation of data protection and the General Data Protection Regulation (hereinafter referred to as the GDPR), which enters into force on May 24<sup>th</sup>, 2018, entail the liability of the controller in breaching the data protection requirements, which in severe cases may entail high monetary penalties. Therefore, at this time it is essential to ensure that the rights and obligations of the employment parties are balanced.

The main goal of the Master's thesis has been the ambition to draw-up a comprehensive approach, which would reflect the actual problems of employment nowadays by analysing applicable national and international legislations for the purpose of balancing the employees' right to privacy and data protection to the employer's statutory obligations and legitimate interest. Based on the legal framework and current issues addressed, the Master's thesis also has a practical value by helping employers to create or renew their internal regulations and educate or counsel their employees.

The thesis is based on the hypothesis that, in view of altered working environment, the employer is not able to fulfil the controller's obligations deriving from GDPR as it impedes the exercise of its fundamental right to engage in entrepreneurial activity.

In order to test the hypothesis, the thesis is divided into three chapters, the first of which opens the fundamental concepts and states the conflicting rights of the employee and the employer, which in the broadest sense are the freedom of the employee's private life and the employer's right to engage in entrepreneurial activity that includes the right to control and monitor the employee and its performance.

The second chapter brings out the legal grounds for the processing of personal data in the recruitment process. Considering that the parties are not yet in contractual relationship, as a rule, the legal ground of data processing can only be the consent of the applicant, unless it is stipulated otherwise by the law (for example in some fields of work the note from Penalty Registry is required). As revealed in the study carried out by K. Visamaa in her bachelor's



paper, many employers use social media to do background checks on the applicants or use the information gathered as a preparation for job interview. Given the widespread use of social media, in summer of 2017, the European Data Protection Working Party considered it vital to issue guidelines to employers, emphasising that, even if a person has a publicly available profile on a social network, the employer should not use them in the recruitment process. The Working Party totally deplores becoming "friends" with the applicant in social media for the purpose of gathering even more information. Despite of that if the employer still has gathered publicly available information about the applicant, the employer undertakes to inform the applicant of the scope and the composition of the information gathered. The corresponding obligation is also stated in art 14 of the GDPR.

The employer's right to engage in entrepreneurial activity also includes the right to choose its employees. Given the employer's goal of profitability, the employer's main interest is to find a skilled worker who shares the values of the company and also fits with the existing team. An interesting aspect of the K. Visamaa's bachelor's thesis is that, even if the employer does not have anything against a person who is actively engaged in social media, such a connection could create discomfort in some of the company's most conservative clients. In order to safeguard their interests, the employer therefore often needs information regarding the applicant even before deciding to invite him/her to the job interview. Although the right to receive information as such is guaranteed by the Constitution, in the context of the GDPR, it would be considered as unlawful data processing, which could be prevented only by informing the applicant about the gathered data. However, in case where the applicant has publicly disclosed his/hers personal data and private life on the Internet, it seems somewhat incomprehensible and undoubtedly burdensome for the employer, which is why the balance between the rights of the data subject and the rights and obligations of the controller are not resolved.

In light of relevant judgement by the District Court of Tallinn, the author explains the necessity and scope of applicant's consent regarding collecting information from previous employers. Based on the recommendations of European Data Protection Party and Estonian Data Protection Inspectorate the author suggests retaining the recruitment materials until the expiry of limitation period for claims. For example according to the Equal Treatment Act the limitation period is one year from the date when the injured party becomes aware or should

become aware of the damage caused. Also taking into account the moderate pace of court proceedings it could be suitable to keep the materials for approximately one and a half year.

The third chapter focuses on a work environment that was altered by ICT developments and socioeconomic changes, including the implementation of monitoring online communication. By entering into contract the parties have agreed to take mutual obligations. According to the very first clause of the Employment Contracts Act the employee commits to work in favour of the employer in subordination to the management and control of the employer. Third clause stipulates the equal treatment principle for the employer and clause 28 sec. 2 sub sec. 11 stipulates the employer's obligation to respect employee's privacy and verify the performance of his or her duties in a manner which does not violate the employee's fundamental rights. Therefore controlling and monitoring the performance of the employees is in itself a legitimate activity, but the employer must first establish sufficient internal rules that cover the possibility of monitoring and also its scope; introduce the rules to the employees and take measures that would minimise the threat to employees' privacy.

The author referred to G. Kempel and H. Urbel's Master's theses, which stipulated that employee's misuse of social media during the off-hours could cause much more severe problems than occupational communication. The Master's thesis highlighted a number of cases in private and public employment relationships, where the employee's inappropriate social media posts or other Internet communications caused a major reputable damage to the company. The author of this thesis shares the view that, just as employees do not leave their private lives behind the door when they go to work, outside of working hours they are bound to the employer as well, and they undertake to share the same values with the employer, keep business secrets and follow a restriction of competition. However, for objective reasons, the employer is not in a position to exercise control over the communication of the employee's private channels thus the negative cases will become public only due to media coverage or by chance.

The thesis also stipulates that telecommuting is gaining more and more popularity, but the employer has no control over it. For example the Occupational Health and Safety Act undertakes the employer to provide a safe working environment, however compliance with this obligation is complicated in a situation where the place of work is the employee's home,

which by the Constitution is inviolable. Therefore the employer has not much to say on the working conditions and environment at employee's home, but could still be held liable in case of occupational accidents or diseases. In view of that, the author of the thesis finds that the employers should still compose and implement some ground rules before allowing telecommuting, so that the requirements and obligations deriving from the Health and Safety Act would be fulfilled at least to the minimal.

The other problem with telecommuting is that there is no possibility to grant the employees' obligation to stay loyal, especially when the employee is working on his/her personal computer, because obviously the employer has no access to it. Without any rules the telecommuting is based only on trust. Therefore the author of this thesis finds that telecommuting protects employees' privacy to the utmost, but the interests of the employer remain unprotected. To balance the rights and obligations, the author finds that the employer should implement internal rules to telecommuting, whereby working in distance should be performed by using employer's devices or servers. And if possible it would be wise to limit telecommuting somehow, for example employee is allowed to work from home office 1-3 days per week.

Processing of special categories of personal data (beliefs, ethnic or racial origin, health data, biometric data, genetic data etc.) in employment is a complicated subject. The processing of such data is permitted by the consent of data subject or as provided by law. Clause 19 of the new Personal Data Protection Act stipulates that processing of special categories of personal data is allowed only if it is strictly necessary in cases of (i) it is provided by the legislation; (ii) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; or (iii) processing relates to personal data which are manifestly made public by the data subject. Most commonly the processing of special categories of personal data in employment is usually with reference to employee's health due to sick or maternity leave and the employer's obligation to organise medical examinations for employees whose health may be affected in the course of the work process, by a working environment hazard or by the nature of the work. It is important to point out that the employer has the right only to receive general information regarding employee's health. Claiming any specifics (diagnoses, medical provisions etc.) is prohibited due to the necessity and minimalism principles.

A quite controversial subject, which has been studied in this thesis, is the employer's obligation derived from the Occupational Health and Safety Act to suspend an employee from work if he/she is under the influence of alcohol, narcotics or toxic or psychotropic substances. The Act compels employer to act in a certain way, but does not give any definition to what can be interpreted as „being under the influence“ nor provide any instructions how to actually act in the situation in a manner that does not harm the employee. Due to the lack of regulation and knowledge employers sometimes use the help of the police, but it can only be done in cases where the employee is clearly under the influence and poses a real threat to other employees or third persons. Based on the judgements of Supreme Court the author of the thesis suggests employers to implement some ground rules and guidelines for fixing the situation and suspending the employee from work.

As working becomes more international the thesis also brings out transatlantic relations regarding employees' personal data and privacy by examining Privacy Shield and applying „whistle-blowing“ concept to Estonian employment practices.

Overall the author finds that hypothesis has been at least partially confirmed. The GDPR obliges the employer, as the controller, to comply with all the principles of processing personal data deriving from the regulation and to introduce various organisational, physical and technological measures for the protection of personal data, while the employer's interests can be undermined or completely overlooked. Therefore the exercise of employer's fundamental right to engage in entrepreneurial activity is being compromised.

## Kasutatud materjalid

### Erialakirjandus

1. Alexy, R. Põhiõigused Eesti põhiseaduses. - Juridica 2001 eriväljaanne. 2001
2. Erlich, S.A, Henberg, A. Kask, O. Põhiseaduse § 31 kommentaarid – Ü.Madise (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017
3. Ernits, M. Põhiseaduse II peatüki kommentaarid - Ü.Madise (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017
4. Ernits, M. Põhiseaduse § 11 kommentaarid - Ü.Madise (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017
5. Henberg, A. Isikuandmete töötlemine töösuhetes. - Juridica VIII/2005
6. Jaanimägi, K. Oja, L. Põhiseaduse § 27 kommentaarid - Ü.Madise (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017
7. Kask, O. Sepp, H. Põhiseaduse § 33 kommentaarid - Ü.Madise (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017
8. Kempel, G. Sotsiaalmeedia töösuhetes: tööandjate hinnangud ja kogemused. Magistritöö. Tartu Ülikool: 2014
9. Kessa, K. Saladuse hoidmise kohustus ja konkurentsipiirang töösuhetes. Magistritöö. Tartu Ülikool: 2013
10. Künnapas, K. Kaugtöö aktuaalseid probleeme. - Juridica IV/2014
11. Mitt, A. Ettevõtlusvabaduse õiguslik olemus. - Juridica VI/2006
12. Ojamäe, E. Töötaja konkurentsikeeld kui lojaalsuskohustus. - Juridica II/2004
13. Urbel, H. Tööle kandideerijate internetipõhine taustauuring ja töötajate monitoorimine: meediaettevõtte näitel. Tartu Ülikool: 2015
14. Tiits, T. Rikkumisest teavitamisega seonduvaid probleeme Eestis. - Juridica VI/2014

### Muu kirjandus:

1. Mereste, U. Majandusleksikon I. Tallinn: Eesti Entsüklopeediakirjastuse AS. 2003

### Ajakirjandus

1. Bershidsky, L. Estonian's Overhyped Silicon Valley. - The Bloomberg View. 05.03.2015. Arvutivõrgus: [https://www.bloomberg.com/view/articles/2015-03-](https://www.bloomberg.com/view/articles/2015-03-05)

05/estonia-s-overhyped-silicon-valley

2. Breadun, D. Whistleblower Bill to Cover Public and Private Sectors. - The Irish Times. 30.01.2012.
3. Himma, M. Eesti elanikud usaldavad kergekäeliselt oma privaatsaid andmeid erinevatele institutsioonidele. - ERR/Novaator. 20.10.2015. Arvutivõrgus: <https://novaator.err.ee/257853/uuring-eesti-elanikud-usaldavad-kergekaeliselt-oma-privaatsaid-andmeid-erinevatele-institutsioonidele>
4. Kaldmäe, L. Kui levinud on Eestis kaugtöö vormis töötamine? – Tööelu portaal. 29.03.2017. Arvutivõrgus: <http://www.tooelu.ee/et/uudised&nID=1514>
1. Kuusik, K. Politseikroonika. - Jõgeva maakonnaleht Vooremaa 17.09.2004
2. Lõugas, H. Privaatsuskilp hakkas tööle: eurooplased saavad andmekaitseks nüüd USA kohtusse pöörduda. - Geenius digiuudiste portaal. 07.12.2016. Arvutivõrgus: <https://geenius.ee/uudis/privaatsuskilp-hakkas-toole-eurooplased-saavad-andmekaitseks-nuud-usa-kohtusse-poorduda/>
3. Nakashima, E. Metadata reveals the secrets of social position, company hierarchy, terrorist cells. - The Washington Post. 15.06.2013. Arvutivõrgus: [https://www.washingtonpost.com/world/national-security/metadata-reveals-the-secrets-of-social-position-company-hierarchy-terrorist-cells/2013/06/15/5058647c-d5c1-11e2-a73e-826d299ff459\\_story.html?noredirect=on&utm\\_term=.b2d5371f754b](https://www.washingtonpost.com/world/national-security/metadata-reveals-the-secrets-of-social-position-company-hierarchy-terrorist-cells/2013/06/15/5058647c-d5c1-11e2-a73e-826d299ff459_story.html?noredirect=on&utm_term=.b2d5371f754b)
4. Peep, V. Kas alati saab Google'ist välja? - Äripäev 19.11.2015.
5. Resmeldt Uusen, R. Eesti personalijuhid paljastavad: kümme elulist trikki, kuidas kandideerides edumaa saavutada. - Postimees. 20.02.2017. Arvutivõrgus: <https://sobranna.postimees.ee/4020765/eesti-personalijuhid-paljastavad-kumme-elulist-trikki-kuidas-kandideerides-edumaa-saavutada>
6. Rooney, B. The Many Reasons Estonia is a Tech Start-up Nation. - The Wall Street Journal. 14.06.2012. Arvutivõrgus: <https://www.wsj.com/articles/SB10001424052702303734204577464343888754210>
7. Süld, R. Biomeetrilise isikutuvastuse levik muudab kogu ühiskonda. - Postimees 03.06.2016. Arvutivõrgus: <https://arvamus.postimees.ee/3719871/rein-suld-biomeetrilise-isikutuvastuse-levik-muudab-kogu-uhiskonda>

## Blogid

1. Liis, M. Andmekaitse inspeksiooni jäik seisukoht raskendab USA börsireeglite

- täitmist. - Advokaadibüroo Eversheds Ots & Co uudisteblogi. 29.03.2016.  
Arvutivõrgus: <https://www.eversheds-sutherland.com/global/en/what/publications/shownews.page?News=en/estonia/ee/Andmekaitse-inspektsiooni-jaik-seisukoht-raskendab-USA>
2. Peers, S. Is Workplace Privacy Dead? Comments on the Barbulescu judgment. - EU Law Analysis õigusblogi. 14.01.2016. Arvutivõrgus: <http://eulawanalysis.blogspot.com/2016/01/is-workplace-privacy-dead-comments-on.html>
  3. Sarmadi, D. Ansip threatens to suspend Safe Harbour data agreement with US. - Euroactive blogi 07.10.2014. Arvutivõrgus: <https://www.euractiv.com/section/innovation-industry/news/ansip-threatens-to-suspend-safe-harbour-data-agreement-with-us/>
  4. Smart, J. Green light for “Big brother” lurking? - Bevan Brittan õigusblogi. 28.01.2016. Arvutivõrgus: <https://www.bevanbrittan.com/insights/articles/2016/ee-green-light-for-big-brother-lurking-investigations-at-work/>

#### Muu meediakajastus

1. Euroopa Komisjoni asepresidendi ja USA asjakohase ametniku ühisavaldus. 19.03.2013 Kättesaadav: <http://2010-2014.commerce.gov/news/press-releases/2012/03/19/us-eu-joint-statement-privacy-eu-commission-vice-president-viviane-re.html>;
2. Euroopa Komisjoni asepresidendi avaldus Justiitsnõukogu kogunemisel Vilniuses. 19.07.2013 Kättesaadav: [http://europa.eu/rapid/press-release\\_MEMO-13-710\\_en.htm](http://europa.eu/rapid/press-release_MEMO-13-710_en.htm);
3. Euroopa Komisjoni pressiteade andmekaitse tähtsusest Euroopas. 28.01.2014 Kättesaadav: [http://europa.eu/rapid/press-release\\_SPEECH-14-62\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm);
4. Euroopa Komisjoni 02.02.2016 pressiteade. Kättesaadav: [http://europa.eu/rapid/press-release\\_IP-16-216\\_en.htm](http://europa.eu/rapid/press-release_IP-16-216_en.htm)
5. Euroopa Komisjoni 12.07.2016 pressiteade Privacy Shield jõustumise kohta. Kättesaadav: [http://europa.eu/rapid/press-release\\_IP-16-2461\\_et.htm](http://europa.eu/rapid/press-release_IP-16-2461_et.htm)

#### Materiaalõigus

1. Ametiühingute seadus. RT I, 12.03.2015, 9
2. Avaliku teenistuse seadus. RT I, 06.10.2016, 2

3. Eesti Vabariigi põhiseadus. RT I, 15.05.2015, 2
4. Individuaalse töövaidluse lahendamise seadus. RT I, 04.06.2014, 5
5. Inimgeeniuringute seadus. RT I, 14.03.2014, 30
6. Inimõiguste ja põhivabaduste kaitse konventsioon. RT II 2000, 11, 57
7. Inimõiguste ülddeklaratsioon.
8. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. RT II 2001, 1, 3
9. Isikuandmete kaitse seadus. RT I, 06.01.2016, 1
10. Karistusseadustik. RT I, 31.12.2016, 14
11. Keskkonnavastutuse seadus. RT I 10.11.2016, 8
12. Krediidiasutuste seadus. RT I, 23.03.2017, 7
13. Korruptsioonivastane seadus. RT I, 24.03.2016, 5
14. Nakkushaiguste ennetamise ja tõrje seadus. RT I, 04.12.2015, 3
15. Politsei- ja piirivalve seadus. RT I, 15.12.2016, 7
16. Ravikindlustuse seadus. RT I, 04.05.2016, 8
17. Raamatupidamise seadus. RT I, 30.12.2015, 65
18. Soolise võrdõiguslikkuse seadus. RT I, 07.07.2015, 11
19. Sotsiaalministri 24.04.2003. a määrus nr 74 “Töötajate tervisekontrolli kord“. RT I, 10.04.2015, 3
20. Tsiviilkohtu menetluse seadustik. RT I, 28.12.2016, 22
21. Töölepinguseadus. RT I, 17.12.2015, 84
22. Töötervishoiu ja tööohutuse seadus. RT I, 08.07.2016, 39
23. Vabariigi Valitsuse 16.05.2013 määrus nr 76 „Riigi personali- ja palgaarvestuse andmekogusse andmete esitamise ja arvestuse toimingute teostamise kord“ RT I, 07.04.2016, 7
24. Vabariigi Valitsuse 26.02.2001 määrus nr. 80 „Asjaajamiskorra ühtsed alused“ § 6 lg 1<sup>1</sup> p. 2. RT I, 26.08.2015, 6
25. Vabariigi Valitsuse 3. aprilli 2008. a määrusega nr 75 “Tööõnnetuse ja kutsuhaigestumise registreerimise, teatamise ja uurimise kord.” RT I, 05.08.2014, 14
26. Võlaõigusseadus RT I, 11.03.2016, 2
27. Võrdse kohtlemise seadus. RT I, 06.07.2012, 22
28. Väärtpaberituru seadus. RT I, 07.04.2017, 4



## Euroopa Liidu õigus

1. Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta ELT L 281/31 24.10.1995
2. Euroopa Liidu Sotsiaalpartnerite raamkokkulepe kaugtöö kohta. 16.02.2002. Arvutivõrgus: [https://www.tooelu.ee/UserFiles/Sisulehtede-failid/Teemad/Kollektiivsed%20t%C3%B6C3%B6suhted/EL\\_sotsiaalpartnerite\\_raamkokkulepete\\_kogumik.pdf](https://www.tooelu.ee/UserFiles/Sisulehtede-failid/Teemad/Kollektiivsed%20t%C3%B6C3%B6suhted/EL_sotsiaalpartnerite_raamkokkulepete_kogumik.pdf)
3. Euroopa Parlamendi ja Nõukogu määrus 2016/679 EL füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta. ELT L 119/1 04.05.2016
4. Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuse täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist. ELT L 119/89 04.05.2016

## Välisriikide õigusaktid

1. Laki naisten ja miesten välisestä tasa-arvosta 609/1986 (Soome)
2. Laki yksityisyyden suojasta työelämässä 759/2004 (Soome)
3. Public Intrests Disclosure Act 1998 (Ühendkuningriik)
4. Sarbanes-Oxley Act of 2002 (USA)
5. Sähköisen viestinnän tietosuojalaki 516/2004 (Soome)
6. Työsopimuslaki luku 55/2001 (Soome)
7. Työterveyshuoltolaki 2001/1383 (Soome)
8. Työturvallisuuslaki 738/2002 (Soome)

## Kohtupraktika

### Tallinna Ringkonnakohus:

1. TlnRnKo 29.02.2016. otsus tsiviilasjas nr 2-15-5896
2. TlnRnKo 17.01.2017 otsus tsiviilasjas nr 2-15-9284

### Riigikohus:

1. RKKKo 3-1-1-134-96 10.12.1996
2. RKPJKo 3-4-1-1-02 06.03.2002
3. RKKKo 3-1-1-102-03 18.09.2003
4. RKHKo 3-3-1-98-06 17.04.2007
5. RKHKo 3-3-1-45-11 26.10.2011
6. RKPJKo 3-4-1-3-12 06.07.2012
7. RKKKo 3-1-1-41-14 01.10.2014
8. RKHKo 3-3-1-13-16 18.10.2016

#### Euroopa Inimõiguste Kohus:

1. 61496/08 *Barbulescu vs Romania* 12.01.2016.
2. 61496/08 *Barbulescu vs Romania* 05.09.2017
3. 62617/00 *Copland vs United Kingdom*. 03.04.2007.
4. 20605/92 *Halford vs United Kingdom*. 25.07.1997.
5. 13710/88 *Niemietz vs Germany* 16.12.1992.
6. 33846/07 *Węgrzynowski and Smolczewski vs Poland* 16.07.2013

#### Euroopa Kohus:

1. Euroopa Kohtu 19.10.2016.a otsus C-582/14 *Breyer vs Saksamaa*
2. Euroopa kohtusse *Digital Rights Ireland* poolt 16.09.2016 esitatud hagi. Kohtuasi T-670/16
3. Euroopa Kohtu 22.11.2017 määrus T-670/16 *Digital Rights Ireland v Commission*
4. Euroopa Kohtu 13.05.2014. otsus C-131/12: *Google Spain SL, Google Inc. versus Agencia de Protección de Datos (AEPD), Mario Costeja González*
5. Euroopa Kohtu 06.10.2015 otsus C-362/14. *Schrems vs Digital Rights Ireland*

#### Juhendid ja soovitused

1. Andmekaitse Inspektsioon. Avaliku teabe seaduse üldjuhend. Tallinn: 2010. Täiendatud märtsis 2016. Arvutivõrgus: [http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/AvTSuldjuhend.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AvTSuldjuhend.pdf)
2. Andmekaitse Inspektsioon. Biomeetriliste isikuandmete töötlemine. Juhendmaterjal. Tallinn, 01.03.2013

3. Andmekaitse Inspeksioon. Isikuandmete töötlemine töösuhetes. Juhendmaterjal. Tallinn 26.05.2014. Arvutivõrgus: [http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/Isikuandmed%20t%C3%B6suhetes%20juhendmaterjal26%2005%202014\\_0.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf)
4. Andmekaitse Inspeksioon. IP-aadress ja privaatsus. Juhendmaterjal. Tallinn, 07.12.2016. Arvutivõrgus: [http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/ip\\_ja\\_privatsus.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ip_ja_privatsus.pdf)
5. Andmekaitse Inspeksioon. Metaandmed ja privaatsus. Juhendmaterjal. Tallinn 2015. Arvutivõrgus: [http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/Juhised/Metaandmed.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/Metaandmed.pdf)
6. Article 29 Data Protection Working Party. Opinion 4/2000 on the level of protection provided by the “Safe Harbor Principles” Brussels, 16.05.2000. Arvutivõrgus: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp32\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf)
7. Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context. Brussels, 13.09.2001. Arvutivõrgus: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf)
8. Article 29 Data Protection Working Party. Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. Brussels 01.02.2006. Arvutivõrgus: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp117\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf)
9. Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Brussels, 20.06.2007. Arvutivõrgus: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf)
10. Article 29 Data Protection Working Party. Opinion 2/2017 on the processing of personal data in the employment context. Brussels, 08.06.2017. Arvutivõrgus: <file:///C:/Users/Liis/Downloads/Opinion22017ondataprocessingatwork-wp249.pdf>
11. Council of Europe. Recommendation CM/Rec(2015) 5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment. Brussels, 01.04.2015. Arvutivõrgus: <https://www.apda.ad/system/files/cm-rec-2015-5-en.pdf>

12. Eesti Standardikeskus. Informatsioon ja dokumentatsioon. Dokumendihaldusprotsessid. Dokumentide metaandmed. EVS-ISO 23081-1
13. Euroopa Nõukogu. Euroopa Liidu Põhiõiguste Amet. Euroopa Andmekaitse Käsiraamat. Luxembourg: Euroopa Liidu Väljaannete Talitus, 2015. Arvutivõrgus: <https://rm.coe.int/16806ae650>
14. Euroopa Komisjoni otsus 26. juuli 2000, 2000/520/EC, vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium. ELT L 215 , 25/08/2000
15. Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus), COM(2012) 11 (final), Brüssel, 25. jaanuar 2012.
16. Euroopa Nõukogu Ministrite Komitee soovitus nr R (89) 2 liikmesriikidele tööhõiveotstarbel kasutatavate isikuandmete kaitse kohta. 1989. Arvutivõrgus: <https://rm.coe.int/16804b8868>
17. Lang, K. I. Pärnamägi, E. Sarapuu (koost.) Avaliku teenistuse seaduse käsiraamat. Justiitsministeerium. Tallinn: 2013. Arvutivõrgus: [https://www.rahandusministeerium.ee/sites/default/files/avaliku\\_teenistuse\\_seaduse\\_kasiraamat\\_0.pdf](https://www.rahandusministeerium.ee/sites/default/files/avaliku_teenistuse_seaduse_kasiraamat_0.pdf)
18. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 23.09.1890. Arvutivõrgus: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>
19. Paragraph 7 of Resolution 1165 of the Parliamentary Assembly of the Council of Europe on the right to privacy. Brussels: 1998. Arvutivõrgus: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16641&lang%20=en>
20. Soolise võrdõiguslikkuse ja võrdse kohtlemise volinik (koost.) Hea Tööandja Teejuht. Juhendmaterjal. 2016. Arvutivõrgus: [http://heatoandja.vordoigusvolinik.ee/wp-content/uploads/2016/03/HeaTooandjaTeejuht\\_60p\\_issuu.pdf](http://heatoandja.vordoigusvolinik.ee/wp-content/uploads/2016/03/HeaTooandjaTeejuht_60p_issuu.pdf)
21. Tööinspeksioon (koost.) Töötaja meelespea. Juhendmaterjal. 2016. Arvutivõrgus: [https://issuu.com/tooinspeksioon/docs/ti\\_vahenenud\\_toovoimega\\_tootaja\\_mee](https://issuu.com/tooinspeksioon/docs/ti_vahenenud_toovoimega_tootaja_mee)
22. United Kingdom Information Commissioner's Office. The Employment Practices Code,

2011. Arvutivõrgus: [https://ico.org.uk/media/for-organisations/documents/1064/the\\_employment\\_practices\\_code.pdf](https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf)

#### Teadusuuringud ja analüüsid

1. Anniste, K. jt. (koost.) Soolise võrdõiguslikkuse seaduse rakendamine Eesti tööandjate seas – uuring 2015. Rakendusuuringu keskus PRAXIS. Tallinn: 2015. Arvutivõrgus: [https://www.sm.ee/sites/default/files/content-editors/Ministeerium\\_kontaktid/Uuringu\\_ja\\_analuusid/Sotsiaalvaldkond/uuringuaruann\\_e.pdf](https://www.sm.ee/sites/default/files/content-editors/Ministeerium_kontaktid/Uuringu_ja_analuusid/Sotsiaalvaldkond/uuringuaruann_e.pdf)
2. Anspal, S. jt. (koost.) Sooline palgalõhe. Sotsiaalministeerium. Tallinn: 2009. Arvutivõrgus: [https://www.sm.ee/sites/default/files/content-editors/Ministeerium\\_kontaktid/Uuringu\\_ja\\_analuusid/Sotsiaalvaldkond/1\\_raport.pdf](https://www.sm.ee/sites/default/files/content-editors/Ministeerium_kontaktid/Uuringu_ja_analuusid/Sotsiaalvaldkond/1_raport.pdf)
3. Eamets, R. Pöder, K. (koost.) Muutuv majandus ja tööturg. Eesti Statistikaamet. Tallinn: 2014. Arvutivõrgus: [file:///C:/Users/Liis/Downloads/Muutuv\\_majandus\\_ja\\_tooturg.pdf](file:///C:/Users/Liis/Downloads/Muutuv_majandus_ja_tooturg.pdf)
4. Eesti Inimõiguste Keskus. Inimõigused Eestis. Inimõiguste aruanne 2007. Tallinn: 2007. Arvutivõrgus: <https://humanrights.ee/materjalid/inimoigused-eestis-2007/>
5. Kaldmäe, L. (toim.) Eesti tööelu uuring 2015. Sotsiaalministeerium. Analüüsi ja statistika osakond. Sotsiaalministeeriumi toimetised. Tallinn: 1/2017. Arvutivõrgus: [https://www.sm.ee/sites/default/files/content-editors/Ministeerium\\_kontaktid/Uuringu\\_ja\\_analuusid/eesti\\_toelu\\_uuring\\_2015.pdf](https://www.sm.ee/sites/default/files/content-editors/Ministeerium_kontaktid/Uuringu_ja_analuusid/eesti_toelu_uuring_2015.pdf)
6. Kallaste, E. Jaakson, K. (koost.) Kaugtöö Eesti organisatsioonides. Eesti Rakendusuuringu Keskus Centar. Tallinn: 2009. Arvutivõrgus: <https://www.riigikantselei.ee/valitsus/valitsus/et/riigikantselei/strateegia/poliitika-analuusid-ja-uuringud/tarkade-otsuste-fondi-strateegiliste-arendusprojektide/Kaugt%C3%B6Eesti%20organisatsioonides.pdf>
7. Nyman Metcalf, K. Privaatsusõigus inimõigusena ja igapäevatehnoloogiad. Tartu Ülikool Ühiskonnateaduste Instituut ja Eesti Inimõiguste Instituut. 2014. Arvutivõrgus: [https://www.humanrightsestonia.ee/inimoiguste\\_uuringud/privaatsus-inimoigusena-ja-igapaevatehnoloogiad/](https://www.humanrightsestonia.ee/inimoiguste_uuringud/privaatsus-inimoigusena-ja-igapaevatehnoloogiad/)
8. Office of the Privacy Commissioner of Canada . What an IP Address Can Reveal About You. A report prepared by the Technology Analysis Branch of the Office Privacy Commissioner of Canada. Quebec: May 2013. Arvutivõrgus:

[https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip\\_201305/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/)

9. Sotsiaalministeerium (tellija). Soolise võrdõiguslikkuse monitooring 2016. Elanikkonna küsitlusuuringute raport. Tallinn: November 2016. Arvutivõrgus: [https://enut.ee/files/soolise\\_vordoiguslikkuse\\_monitooringu\\_raport\\_2016.pdf](https://enut.ee/files/soolise_vordoiguslikkuse_monitooringu_raport_2016.pdf)

#### Seaduse eelnõude seletuskirjad

1. Avaliku teenistuse seaduse eelnõu 193 SE (2012) seletuskiri
2. Isikuandmete kaitse seaduse eelnõu 1026 SE (2006) seletuskiri.
3. Isikuandmete kaitse seaduse eelnõu SE 616 (2018) seletuskiri
4. Töölepingu seaduse eelnõu 299 SE (2008) seletuskiri

#### Ametlikud veebilehed

1. Andmekaitse Inspektsiooni koduleht. Kättesaadav: [www.aki.ee](http://www.aki.ee)
2. Euroopa Inimõiguste Kohtu kodulehekülg. Kättesaadav: [www.echr.coe.int](http://www.echr.coe.int)
3. Justiitsministeeriumi koduleht. Kättesaadav: [www.just.ee](http://www.just.ee)
4. Riigi Infosüsteemide Ameti kodulehekülg. Kättesaadav: [www.ria.ee](http://www.ria.ee)
5. Tööinspektsiooni koduleht. Kättesaadav: [www.ti.ee](http://www.ti.ee)
6. Viimsi valla koduleht. Kättesaadav: [www.viimisvald.ee](http://www.viimisvald.ee)

#### Muu materjal

1. CV Online kasutustingimused. Kättesaadav: [www.cv.ee/terms/seeker/](http://www.cv.ee/terms/seeker/)
2. Hollandi väärkäitumisest teatamise infolehekülg *Adviespunt Klokkenluiders* kättesaadav: [www://huisvoorklokkenluiders.nl/](http://www://huisvoorklokkenluiders.nl/)
3. MeetFrank OÜ kodulehekülg. Kättesaadav: [www.meetfrank.ee](http://www.meetfrank.ee)
4. Telia Eesti AS koduleht. Kättesaadav: [www.telia.ee](http://www.telia.ee)
5. Talentest OÜ kodulehekülg. Kättesaadav: [www.talentest.ee](http://www.talentest.ee)

## **Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks**

Mina, Liis Miller

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

### **Lepingupoolte õiguste tasakaalustamine kaasaegsetes töösuhetes andmekaitse üldmääruse kontekstis,**

mille juhendaja on LLM Mari Männiko

- 1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
- 1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace'i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.
3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, 23.04.2018