EUROOPA
KOMISJON

Brüssel, 29.5.2019
COM(2019) 250 final

KOMISJONI TEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE

Suunised määruse kohta, mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku

Sisukord

1. Sissejuhatus

Kuna majandus muutub üha andmepõhisemaks, on andmevood kõigis valdkondades tegutsevate mis tahes suurusega ettevõtjate äriprotsesside alus. Uued digitaaltehnoloogiad annavad uusi võimalusi üldsusele, ettevõtjatele ja haldusasutustele Euroopa Liidus (edaspidi „EL“).

Selleks et veelgi suurendada piiriülest andmevahetust ja elavdada andmepõhist majandust, võtsid Euroopa Parlament ja nõukogu Euroopa Komisjoni (edaspidi „komisjon“) ettepaneku alusel novembris 2018 vastu määruse (EL) 2018/1807, mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku[1] (edaspidi „isikustamata andmete vaba liikumise määrus“). Nimetatud määrust hakatakse kohaldama 28. maist 2019. Isikuandmete vaba liikumise põhimõte on juba sätestatud määruses (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)[2]. Selle tulemusena on nüüd olemas terviklik raamistik ühtse Euroopa andmeruumi ja kõigi andmete vaba liikumise jaoks ELis[3].

Isikustamata andmete vaba liikumise määrus annab ettevõtjatele õiguskindluse, et nad võivad oma andmeid töödelda kõikjal ELis, suurendab usaldust andmetöötlusteenuste vastu ja aitab vältida seotust ühe pakkujaga. See suurendab tarbijate valikuvõimalusi, parandab tõhusust ning stimuleerib pilvtehnoloogia kasutuselevõttu, mis võimaldab ELi ettevõtjatel märkimisväärselt kulusid kokku hoida. Ühe uuringu kohaselt saavad ELi ettevõtjad pilvteenuseid kasutusele võttes vähendada oma IT-kulusid 20–50 %[4].

Tänu neile kahele määrusele saavad andmed liikmesriikide vahel vabalt liikuda ning andmetöötlusteenuste kasutajad saavad kasutada eri ELi turgudel kogutud andmeid, et parandada oma tootlikkust ja konkurentsivõimet. Seeläbi saavad kasutajad täiel määral kasu ELi turu suurusest tulenevast mastaabisäästust, mis parandab nende ülemaailmset konkurentsivõimet ja suurendab Euroopa andmepõhise majanduse ühendatust.

Isikustamata andmete vaba liikumise määrusel on kolm märkimisväärset omadust:

- sellega keelatakse liikmesriikidel reeglina kehtestada nõudeid andmete asukohale. Sellest reeglist võidakse teha erandeid üksnes avaliku julgeoleku kaalutlustel kooskõlas proportsionaalsuse põhimõttega;

---

[1] Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määrus (EL) 2018/1807, mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku (ELT L 303, 28.11.2018, lk 59).

[2] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

[3] Isikuandmete kaitse üldmäärus hõlmab ka Euroopa Majanduspiirkonda (edaspidi „EMP“), kuhu kuuluvad Island, Liechtenstein ja Norra. Lisaks sellele on isikustamata andmete vaba liikumise määrus märgitud EMPs kohaldatavaks.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe*, SMART 2014/0031, 2016. Kättesaadav aadressil: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

- sellega luuakse koostöömehhanism, millega tagatakse, et pädevatele asutustele jääb õigus saada juurdepääs vajalikele andmetele ka siis, kui neid hakatakse töötlema teises liikmesriigis;
- sellega antakse tööstussektorile ajend töötada komisjoni toetusel välja iseregulatsiooni tegevusjuhendid, mis käsitlevad teenuseosutajate vahetamist ja andmete portimist.

Käesolevate suuniste eesmärk

Käesolevad suunised on koostatud, et täita isikustamata andmete vaba liikumise määruse artikli 8 lõikes 3 esitatud nõuet avaldada suunised, milles käsitletakse nimetatud määruse ja isikuandmete kaitse üldmääruse koostoimet, „eelkõige selliste andmekogude puhul, mis sisaldavad nii isikuandmeid kui ka isikustamata andmeid.“

Käesolevate suuniste eesmärk on aidata kasutajatel – eelkõige väikestel ja keskmise suurusega ettevõtjatel – mõista isikustamata andmete vaba liikumise määruse ja isikuandmete kaitse üldmääruse koostoimet[5]. Seetõttu käsitlevad suunised eelkõige: i) isikustamata andmete ja isikuandmete kontseptsiooni, ii) andmete vaba liikumise põhimõtet ja andmete asukohale nõuete esitamise keeldu mõlema määruse alusel ning iii) andmete porditavuse (ülekantavuse) kontseptsiooni isikustamata andmete vaba liikumise määruse alusel. Samuti käsitletakse suunistes nende kahe määrusega kehtestatud iseregulatsiooni nõudeid.

Isikustamata andmete vaba liikumise määrus käsitleb ainult „muid andmeid kui isikuandmeid“, mis on määratletud isikuandmete kaitse üldmääruses. Isikuandmete kaitse üldmäärusega reguleeritakse isikuandmete töötlemist, mis on ELi andmekaitseraamistiku[6] oluline osa. Määrus jõustus liikmesriikides 25. mail 2018. Sellega kehtestatakse ühtlustatud normid, millega kaitstakse ELis/EMPs elavaid inimesi nende isikuandmete töötlemise ja nende andmete vaba liikumise puhul. Isikuandmete kaitse üldmäärusega: i) täpsustatakse, millise teabe puhul on tegu isikuandmetega, ii) kehtestatakse nende andmete töötlemise õiguslik alus ning iii) määratletakse muu hulgas õigused ja kohustused, mida tuleb järgida

[5] Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) põhjendus 37.

[6]
- Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).
- Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).
- 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 ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (ELT L 119, 4.5.2016, lk 89).
- Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37) (praegu läbivaatamisel).

nende andmete töötlemisel,[7]. Isikuandmete vaba liikumise põhimõtte kohta on isikuandmete kaitse üldmääruse artikli 1 lõikes 3 sätestatud, et „[i]sikuandmete vaba liikumist liidus ei piirata ega keelata põhjustel, mis on seotud füüsiliste isikute kaitsega isikuandmete töötlemisel“.

Tegelikkuses koosneb andmekogu üldjuhul nii isikuandmetest kui ka isikustamata andmetest. Sellist andmekogu nimetatakse sageli segaandmekoguks. Punktis 2.2 allpool selgitatakse täpsemalt isikustamata andmete vaba liikumise määruse ja isikuandmete kaitse üldmääruse koostoimet segaandmekogude puhul.

Selguse huvides olgu öeldud, et isikuandmete kaitse üldmääruses ja isikustamata andmete vaba liikumise määrusega ei ole kehtestatud üksteisega vastuolus olevaid kohustusi.

2. Isikustamata andmete vaba liikumise määruse ja isikuandmete kaitse üldmääruse koostoime – segaandmekogud

2.1. Isikustamata andmete kontseptsioon isikustamata andmete vaba liikumise määruses

Isikustamata andmete vaba liikumise määruse[8] eesmärk on tagada muude andmete kui isikuandmete vaba liikumine. Määruses kasutatakse läbivalt mõistet „andmed“, mille määratlus on „muud andmed kui isikuandmed, mis on määratletud määruse (EL) 2016/679 [isikuandmete kaitse üldmäärus] artikli 4 punktis 1“[9]. Need andmed, millele osutatakse käesolevas dokumendis ka kui „**isikustamata andmetele**“ on määratletud vastandina isikuandmetele, mille määratlus on esitatud isikuandmete kaitse üldmääruses.

Isikuandmed

Isikuandmete kaitse üldmääruse kohaselt: on isikuandmed „igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme

---

[7] Täiendavaid suuniseid Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) ja Euroopa andmekaitsealaste õigusaktide eri aspektide kohta leiate Euroopa Andmekaitsenõukogu veebilehel, kus on esitatud mitmeid suuniseid vastavalt isikuandmete kaitse üldmääruse artiklile 70: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_et. Sellel veebilehel on osutatud ka Euroopa Andmekaitsenõukogu eelkäija – artikli 29 töörühma – suunistele, soovitustele ja muudele dokumentidele. Selleks et suurendada kodanike ja ettevõtjate teadlikkust Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrusest (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)), avaldas komisjon andmekaitsealase teatise, milles esitatakse suunised isikuandmete kaitse üldmääruse vahetu kohaldamise kohta (COM/2018/043 final), mis on saadaval aadressil: https://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

[8] Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) artikkel 1.

[9] Vt Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) artikli 3 punkt 1.

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

Isikuandmete määratlus on tahtlikult lai ja see on jäänud isikuandmete kaitse üldmääruses võrreldes varasemate õigusaktidega sisuliselt muutumatuks[10]. Isikuandmete määratluse eri aspekte, näiteks „igasugune teave“, „tuvastatud või tuvastatava“, „kohta“, käsitles juba artikli 29 töörühm[11] oma 20. juuni 2007. aasta arvamuses 4/2007 isikuandmete mõiste kohta, WP 136.

Sellistes valdkondades nagu teadusuuringud on tavapärane pseudonüümida isikuandmed, et varjata isiku identiteeti. **Pseudonüümimine** on isikuandmete töötlemine, mille tulemusena pole võimalik omistada neid konkreetsele isikule ilma lisateavet kasutamata. Seda lisateavet hoitakse eraldi ja kaitstakse organisatsiooniliste või tehnoloogiliste meetodite (näiteks krüpteerimise) abil[12][13]. Pseudonüümitud andmeid käsitatakse sellest hoolimata andmetena tuvastatava isiku kohta, kui neid saab omistada sellele isikule lisateabe abil[14]. Vastavalt isikuandmete kaitse üldmäärusele on sellised andmed **isikuandmed**.

Isikustamata andmed

Kui andmed ei ole isikuandmete kaitse üldmääruses määratletud „isikuandmed“, siis on tegemist **isikustamata andmetega**. Isikustamata andmeid saab liigitada päritolu põhjal järgmiselt:

- esiteks: andmed, mis ei olnud algselt seotud tuvastatud või tuvastatava füüsilise isikuga, näiteks tuulegeneraatoritele paigaldatud anduritest saadud andmed ilmastikutingimuste kohta või andmed tööstuslike masinate hooldamise vajaduse kohta;

[10] Vt Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ (üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta) artikli 2 punkt a (määrus kaotas kehtivuse 24. mail 2018, kui see tunnistati kehtetuks isikuandmete kaitse üldmäärusega). Vt ka Euroopa Kohtu isikuandmete määratlust käsitlevaid kohtulahendeid, millega tunnustatakse selle mõiste laia tõlgendust, näiteks Euroopa Kohtu 29. jaanuari 2009. aasta otsus kohtuasjas Productores de Música de España (Promusicae) *vs.* Telefónica de España SAU, C-275/06, ECLI:EU:C:2008:54; Euroopa Kohtu 24. novembri 2011. aasta otsus kohtuasjas Scarlet Extended SA *vs.* Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, ECLI:EU:C:2011:771; Euroopa Kohtu 19. oktoobri 2016. aasta otsus kohtuasjas Patrick Breyer *vs.* Saksamaa Liitvabariik, C-582/14, ECLI:EU:C:2016:779.

[11] Artikli 29 töörühm oli nõustamisorgan, mis andis komisjonile nõu andmekaitseküsimustes ja aitas välja töötada ELi ühtlustatud andmekaitsepoliitikat. Pärast isikuandmete kaitse üldmääruse jõustumist 25. mail 2018 asus artikli 29 töörühma asemel tegutsema Euroopa Andmekaitsenõukogu.

[12] Pseudonüümimise mõiste on määratletud Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) artikli 4 punktis 5 (seal on kasutatud terminit „pseudonümiseerimine“).

[13] Näiteks uue ravimi mõju käsitleva teadusuuringu võib lugeda pseudonüümituks, kui uuringus osalejate isikuandmed asendatakse uuringudokumentides kordumatu atribuudiga (näiteks numbri või koodiga) ning nende isikuandmeid hoitakse määratud kordumatutest atribuutidest eraldi turvatud dokumendis (näiteks salasõnaga kaitstud andmebaasis).

[14] Vt Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) põhjendus 26.

- teiseks: andmed, mis olid algselt isikuandmed, aga mis hiljem **anonüümiti**[15]. Isikuandemete „anonüümimine“ erineb eespool kirjeldatud pseudonüümimisest, kuna nõuetekohaselt anonüümitud andmeid ei saa omistada konkreetsele isikule isegi lisaandmeid kasutades[16] ja seetõttu on tegemist isikustamata andmetega.

Andmete nõuetekohast anonüümimist hinnates lähtutakse iga konkreetse juhtumi eriomastest ja ainulaadsetest asjaoludest[17]. Mitmed juhtumid, mille puhul on väidetavalt anonüümitud andmekogude alusel isikud uuesti kindlaks tehtud, näitavad, et see hindamine võib olla keeruline[18]. Isiku tuvastatavuse kindlaks tegemiseks tuleb uurida kõiki võimalusi, mida vastutav töötleja või muu isik võib mõistlikult kasutada, et isik otseselt või kaudselt tuvastada[19].

Isikustamata andmete näited

- Andmeid, mis on koondatud üksikute sündmuste (näiteks isiku konkreetsed reisid välismaale või reisimisharjumused, mida võiks pidada isikuandmeteks) tuvastamist mittevõimaldaval viisil, võib pidada anonüümseteks andmeteks[20]. Anonüümseid andmeid kasutatakse näiteks statistikas või müügiaruannetes (näiteks toote ja selle funktsioonide populaarsuse hindamiseks).
- Finantssektori sagedase kauplemise andmed või andmed täppispõllumajanduse kohta, mis aitavad jälgida ning optimeerida pestitsiidide, toitainete ja vee kasutust.

---

[15] Vt Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) põhjendus 26, milles on sätestatud, et „[a]ndmekaitse põhimõtteid ei tuleks seetõttu kohaldada anonüümse teabe suhtes, nimelt teave, mis ei ole seotud tuvastatud või tuvastatava füüsilise isikuga, või isikuandmete suhtes, mis on muudetud anonüümseks sellisel viisil, et andmesubjekti ei ole võimalik tuvastada või ei ole enam võimalik tuvastada.“

[16] Vt Euroopa Kohtu 19. oktoobri 2016. aasta otsus kohtuasjas Patrick Breyer *vs.* Saksamaa Liitvabariik, C-582/14, ECLI:EU:C:2016:779. Euroopa Kohus otsustas, et dünaamilist IP-aadressi võidakse käsitada isikuandmetena isegi juhul, kui kolmandal isikul (näiteks internetiteenuse osutajal) on täiendavad andmed, mille abil on võimalik isik tuvastada. Isiku tuvastamise võimalus peab olema selline, mida võidakse mõistliku tõenäosusega kasutada isiku otseseks või kaudseks tuvastamiseks.

[17] Andmete anonüümimiseks tuleks alati kasutada uusimaid tehnika tasemel anonüümimismeetodeid.

[18] Eeldatavalt anonüümitud andmete põhjal isikute tuvastamise näiteid leiate Euroopa Parlamendi tööstuse, teadusuuringute ja energeetikakomisjoni tehtud uuringust tulevaste andmevoogude kohta, mille koostasid Blackman, C. ja Forge, S.: *„Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee“,* 2017, lk 22, tekstikast 2. Kättesaadav aadressil: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

[19] Vt isikuandmete kaitse üldmääruse (EL) 2016/679 põhjendus 26, mille kohaselt tuleks selleks, „et teha kindlaks, kas füüsilise isiku tuvastamiseks võetakse mõistliku tõenäosusega meetmeid, [...] arvestada kõiki objektiivseid tegureid, näiteks tuvastamise maksumus ja selleks vajalik aeg, võttes arvesse nii andmete töötlemise ajal kättesaadavat tehnoloogiat kui ka tehnoloogilisi arenguid.“

[20] Vt artikli 29 töörühma *arvamus 05/2014 anonüümimistehnikate kohta*, vastu võetud 10. aprillil 2014 (WP216), lk 9: „Üksnes juhul, kui vastutav töötleja üldistab andmeid sedavõrd, et üksikud sündmused ei ole enam tuvastatavad, võib saadud andmekogumit käsitleda anonüümsena. Näiteks kui organisatsioon kogub üksikisikute reisiandmeid, kvalifitseeruvad üksikisikute reisimarsruudid sündmuse tasandil kõigi osaliste jaoks endiselt kui isikuandmed seni, kuni vastutaval töötlejal (või muul osalejal) on juurdepääs algsetele toorandmetele, isegi kui vahetud tunnusandmed on kolmandate isikute jaoks ette nähtud andmetest eemaldatud. Kui aga vastutav töötleja kustutab toorandmed ning esitab kolmandatele isikutele kõrgel tasemel üksnes üldistatud statistika, näiteks et „Esmaspäeviti on trajektooril X 160 % rohkem reisijaid kui teisipäeviti“, siis see kvalifitseerub anonüümse teabena.“

Kuid kui isikustamata andmed võivad olla seotud üksikisikuga ükskõik mis viisil, mille tulemusena muutub isik kas otseselt või kaudselt tuvastatavaks, siis tuleb andmeid käsitada isikuandmetena.

Näiteks kui tootmisliini kvaliteedikontrolli aruanne võimaldab seostada andmeid tehase konkreetsete töötajatega (näiteks nendega, kes määrasid kindlaks tootmisparameetrid), siis on need andmed isikuandmed, mille suhtes tuleb kohaldada isikuandmete kaitse üldmäärust. Samad reeglid kehtivad juhul, kui tehnoloogia ja andmeanalüüsi areng võimaldab muuta anonüümitud andmed isikuandmeteks. [21]

Kuna isikuandmete määratlus osutab füüsilistele isikutele, on juriidiliste isikute nimesid ja kontaktandmeid sisaldavate andmekogude puhul põhimõtteliselt tegemist isikustamata andmetega[22]. Kuid teatavates olukordades võivad need olla isikuandmed[23]. Seda näiteks juhul, kui juriidilise isiku nimi on sama kui selle omanikuks oleva füüsilise isiku nimi või kui teave sisaldab andmeid tuvastatud või tuvastatava füüsilise isiku kohta[24].

2.2. Segaandmekogud

Isikustamata andmete vaba liikumise määrus ja isikuandmete kaitse üldmäärus käsitlevad andmete vaba liikumist ELis kahest vaatekohast.

Isikustamata andmete vaba liikumise määrusega kehtestatakse üldine keeld esitada nõudeid isikustamata andmete asukohale. Määruse artikli 4 lõikega 1 keelatakse esitada nõudeid andmete asukohale, välja arvatud juhul, kui need on põhjendatud avaliku julgeoleku kaalutlustel ja kooskõlas proportsionaalsuse põhimõttega.

Isikuandmete kaitse üldmäärusega tagatakse lisaks isikuandmete kõrgetasemelisele kaitsele ka nende vaba liikumine. Määruse artikli 1 lõikes 3 on sätestatud, et „[i]sikuandmete vaba liikumist liidus ei piirata ega keelata põhjustel, mis on seotud füüsiliste isikute kaitsega isikuandmete töötlemisel“. Ühiselt sätestavad need kaks määrust kõigi andmete vaba liikumise ELis. Erisätteid käsitletakse täpsemalt punktides 3.1 ja 3.2.

---

[21] Kui isikuandmeid töödeldakse ebaseaduslikult või nende töötlemisega rikutakse muul moel isikuandmete kaitse üldmääruse nõudeid, siis on andmesubjektidel (füüsilistel isikutel) õigus esitada isikuandmete kaitse üldmääruse alusel kaebus riiklikule järelevalveasutusele (andmekaitseasutusele) ELis või pöörduda tõhusate õiguskaitsemeetmete võtmiseks liikmesriigi kohtusse. Riiklike järelevalveasutuste pädevust, ülesandeid ja volitusi reguleerib isikuandmete kaitse üldmääruse VI peatüki 2. jagu.

[22] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) põhjenduses 14 on sätestatud, et „[ü]kski isik ei peaks nõudma käesoleva määrusega ette nähtud kaitset seoses selliste andmete töötlemisega, mis puudutavad juriidilisi isikuid, eelkõige juriidiliste isikutena asutatud ettevõtjaid, sealhulgas juriidilise isiku nime ja vormi ning kontaktandmeid.“ Seda põhjendust lugedes tuleb siiski võtta arvesse isikuandmete kaitse üldmääruse artikli 4 punktis 1 esitatud isikuandmete määratlust.

[23] Vt Euroopa Kohtu 9. novembri 2010. aasta otsus ühendatud kohtuasjades Volker und Markus Schecke GbR, C-92/09 ning Hartmut Eifert, C-93/09 *vs.* Land Hessen, ECLI:EU:C:2010:662, punkt 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_et

Segaandmekogu koosneb nii isiku- kui ka isikustamata andmetest. Enamik andmepõhises majanduses kasutatavatest andmekogudest on segaandmekogud, mis on levinud selliste tehnoloogiliste uuenduste tõttu nagu asjade internet (s.o objektide digitaalne ühendamine), tehisintellekt ja suurandmete analüüsi võimaldavad tehnoloogiad.

Segaandmekogude näited

- Ettevõtte maksuaruanne, mis sisaldab ettevõtte direktori nime ja telefoninumbrit;
- panga andmekogud, eelkõige need, mis sisaldavad kliendi- ja tehinguandmeid, näiteks makseteenused (krediit- ja deebetkaardid), partnerisuhete haldamise (PRM) rakendused, laenulepingud ja dokumendid, mis sisaldavad andmeid nii füüsiliste kui ka juriidiliste isikute kohta;
- teadusasutuse anonüümitud statistilised andmed ja algselt kogutud toorandmed, näiteks üksikisikute vastused statistilise uuringu küsimustele;
- ettevõtte IT-probleeme ja nende lahendusi sisaldav teadmiste andmebaas, mis põhineb konkreetsete IT-intsidentide aruannetel;
- asjade internetiga seotud andmed, millest mõned võimaldavad teha järeldusi tuvastatavate isikute kohta (näiteks konkreetsel aadressil viibimise ja seadme kasutamise seaduspärad), ning
- tööstuse tootmisseadmete operatiivlogi andmete analüüs.

Näide: kliendisuhte haldamise teenused

Mõned pangad kasutavad kolmandate isikute pakutavaid kliendisuhete haldamise (CRM) teenuseid, mille puhul tuleb teha kliendiandmed kättesaadavaks CRMi keskkonnas. CRMi teenuses hoitavad andmed sisaldavad teavet, mis on vajalik, et hallata tulemuslikult suhtlust klientidega, näiteks nende postiaadressi ja e-posti aadressi, telefoninumbrit, nende ostetavaid tooteid ja teenuseid ning müügiaruandeid, sh koondandmeid. Need andmed võivad seega sisaldada nii isiku- kui ka isikustamata andmeid.

Segaandmekogude kohta on isikustamata andmete vaba liikumise määruses[25] sätestatud järgmist:

„Nii isikuandmeid kui ka isikustamata andmeid sisaldavate andmekogude puhul kohaldatakse käesolevat määrust andmekogu isikustamata andmete osa suhtes. Kui andmekogus on isikuandmed ja isikustamata andmed lahutamatult seotud, ei piira käesolev määrus määruse (EL) 2016/679 kohaldamist.“

See tähendab, et nii isiku- kui ka isikustamata andmeid sisaldavate andmekogude puhul

- kohaldatakse andmekogu isikustamata andmete osa suhtes isikustamata andmete vaba liikumise määrust,

[25] Artikli 2 lõikes 2.

- kohaldatakse andmekogu isikuandmete osa suhtes isikuandmete kaitse üldmääruse andmete vaba liikumise sätet[26] ning
- kui isikustamata ja isikuandmete osa on omavahel lahutamatult seotud, siis kohaldatakse kogu segaandmekogu suhtes täielikult isikuandmete kaitse üldmäärusest tulenevaid andmekaitseõigusi ja -kohustusi isegi juhul, kui isikuandmed moodustavad ainult andmekogu väikse osa[27].

See tõlgendus on kooskõlas isikuandmete kaitse õigusega, mille tagab Euroopa Liidu põhiõiguste harta,[28] ja isikustamata andmete vaba liikumise määruse[29] põhjendusega 8. Põhjenduses 8 on sätestatud, et „[k]äesolev määrus ei mõjuta õigusraamistikku, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel, [...] eelkõige [isikuandmete kaitse üldmäärust] ning [...] direktiive (EL) 2016/680 ja 2002/58/EÜ.“

Praktiline näide

ELis tegutsev ettevõtja pakub platvormi kaudu oma teenuseid. Ettevõtjad (kliendid) laadivad platvormi üles oma dokumendid, mis sisaldavad segaandmekogusid. Dokumente üles laadiv ettevõtja peab vastutava töötlejana veenduma, et andmete töötlemine on kooskõlas isikuandmete kaitse üldmäärusega. Kui teenust pakkuv ettevõtja (volitatud töötleja) töötleb andmekogu vastutava töötleja nimel, siis peab ta salvestama ja töötlema andmeid kooskõlas isikuandmete kaitse üldmäärusega, näiteks veenduma, et tagatakse andmete turvalisuse nõuetekohane tase, sealhulgas krüpteerimise teel.

Lahutamatu seotuse mõistet ei ole määratletud kummaski määruses[30]. See võib tegelikkuses osutada olukorrale, kus andmekogu sisaldab isiku- ja isikustamata andmeid ning nende kahe andmete tüübi eraldamine oleks kas võimatu või vastutava töötleja arvates majanduslikult ebaotstarbekas või tehniliselt teostamatuks. Näiteks peaks ettevõtja CRMi ja müügiaruandluse süsteemide ostmisel tegema tarkvara omandamiseks topeltkulutused, ostes eraldi tarkvara CRMi (isikuandmed) ja CRMi andmetel põhinevate müügiaruandluse süsteemide (koondandmed / isikustamata andmed) jaoks.

Andmekogu andmete eraldamine vähendab ka suure tõenäosusega märkimisväärselt andmekogu väärtust. Pealegi muudab andmete muutuv olemus (vt punkt 2.1) andmete selge eristamise ja andmete erinevate liikide eraldamise palju keerukamaks.

---

[26] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) artikli 1 lõige 3. Vt ka käesoleva dokumendi punkt 3.2.

[27] Nagu toodi esile *komisjoni talituste töödokumendis „Mõjuhinnang, mis on lisatud dokumendile „Euroopa Parlamendi ja nõukogu määrus, mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku““* (SWD(2017) 304 final), osa 1/2, lk 3, „olenemata sellest, kui palju isikuandmeid segaandmekogu sisaldab, tuleb andmekogu isikuandmeid sisaldava osa puhul täielikult järgida isikuandmete kaitse üldmääruse nõudeid.“

[28] Euroopa Liidu põhiõiguste harta (ELT C 362, 26.10.2012, lk 391).

[29] Põhjendus 8.

[30] Isikustamata andmete vaba liikumise määrus ja isikuandmete kaitse üldmäärus.

Tuleb tähele panna, et kumbki määrus ei kohusta ettevõtjaid eraldama andmekogusid, mille vastutavad või volitatud töötlejad nad on.

Seetõttu kohaldatakse segaandmekogu suhtes üldjuhul vastutavate töötlejate ja volitatud töötlejate kohustusi ning selle puhul austatakse andmesubjektide õigusi, mis on kehtestatud isikuandmete kaitse üldmäärusega.

Terviseandmete töötlemine

Segaandmekogu võib sisaldada terviseandmeid. Näiteks elektroonilised tervisekaardid, kliinilised uuringud või mitmesuguste m-tervise ja heaolurakenduste (näiteks rakendused, millega mõõdetakse meie tervislikku seisundit, millega tuletatakse meelde ravimite võtmise vajadust või jälgitakse meie sportlikke saavutusi)[31] kogutud andmekomplektid. Tehnoloogia arengu tõttu on üha keerukam täpselt eristada isiku- ja isikustamata andmeid neis andmekogudes. Seetõttu tuleb nende andmete töötlemisel järgida isikuandmete kaitse üldmäärust, eelkõige artiklit 9 (võttes arvesse, et terviseandmed on selle määruse kohaselt andmete eriliik), milles on sätestatud andmete eriliikide töötlemise üldine keeld ja selle keelu erandid.

Segaandmekogude terviseandmed võivad olla väärtuslik teabeallikas näiteks täiendavateks meditsiiniuuringuteks, määratud ravimi kõrvaltoimete mõõtmiseks, haigustest statistilise ülevaate saamiseks või uute tervishoiuteenuste või ravimeetodite väljatöötamiseks. Kuid andmete esialgse ja täiendava töötlemise käigus tuleb järgida isikuandmete kaitse üldmäärust. Seetõttu peab terviseandmete igasugusel sellisel töötlemisel olema kehtiv õiguslik alus[32] ja nõuetekohane põhjendus, see peab olema turvaline ja selle puhul tuleb tagada piisavad kaitsemeetmed.

Samuti on ülioluline tagada üksikisikutele ja ettevõtjatele õiguskindlus ning usaldus andmete töötlemise vastu. See on hädavajalik ka andmepõhise majanduse huvides. See tagatakse nende kahe määrusega, mille mõlema eesmärk on mitte takistada andmete vaba liikumist.

3. Andmete vaba liikumine ja andmete asukohale esitatavate nõuete kaotamine

Selles punktis selgitatakse üksikasjalikumalt isikustamata andmete vaba liikumise määruses kirjeldatud andmete asukohale esitatavate nõuete kontseptsiooni ja isikuandmete kaitse üldmääruses sätestatud vaba liikumise põhimõtet. Kuigi need sätted on suunatud liikmesriikidele, võivad need olla abiks ettevõtjatele, et nad mõistaksid paremini, kuidas need kaks määrust aitavad tagada kõigi andmete vaba liikumise ELis.

[31] M-tervise rakenduste väljatöötamisel ja käitamisel tuleb rangelt järgida isikuandmete kaitse üldmäärust. Neid nõudeid täpsustatakse m-tervise rakenduste privaatsust käsitlevas tegevusjuhendis, mis on praegu koostamisel. Rohkem teavet selle kohta, kuidas dokumendi koostamine edeneb, leiate veebisaidil: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

[32] Vt Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) artikli 6 lõige 1.

3.1. Isikustamata andmete vaba liikumine

Isikustamata andmete vaba liikumise määruses[33] on sätestatud, et „[a]ndmete asukoha nõuded on keelatud, välja arvatud juhul, kui need on põhjendatud avaliku julgeoleku kaalutlustel ja kooskõlas proportsionaalsuse põhimõttega.“

Andmete asukoha nõue on määratletud[34] kui „kohustus, keeld, tingimus, piirang või muu liikmesriigi õigus- või haldusnormides sätestatud või liikmesriigi ja avalik-õiguslike isikute (sealhulgas riigihangete valdkonnas) üldisest ja järjepidevast haldustavast tulenev nõue, mis ei piira direktiivi 2014/24/EL kohaldamist ja millega nähakse ette andmete töötlemine teatava liikmesriigi territooriumil või millega takistatakse andmetöötlust teises liikmesriigis[35].“

Määratlus näitab, et ELis andmete vaba liikumist piiravad meetmed võivad esineda eri kujul. Need võivad olla kehtestatud seadustes, haldusaktides ja -sätetes või olla üldtunnustatud ja järjepidevate haldustavade tulemus. Lisaks sellele hõlmab andmete asukoha nõuete keeld nii otseseid kui ka kaudseid meetmeid, mis piiraksid isikustamata andmete vaba liikumist.

Otsesed nõuded andmete asukohale võivad näiteks seisneda kohustuses säilitada andmeid konkreetses geograafilises asukohas (näiteks serverid peavad asuma konkreetses liikmesriigis) või kohustuses järgida konkreetseid riiklikke tehnilisi nõudeid (näiteks andmete puhul tuleb kasutada konkreetseid riigiomaseid vorminguid).

Kaudsed nõuded andmete asukohale , mis takistaksid isikustamata andmete töötlemist muus liikmesriigis, võivad esineda mitmel kujul. Näiteks võidakse nõuda konkreetses liikmesriigis sertifitseeritud või kinnitatud tehnorajatiste kasutamist või esitada muid nõudeid, mille tõttu on raskem töödelda andmeid väljaspool teatavat Euroopa Liidu geograafilist piirkonda või territooriumi[36,37].

Kui hinnatakse, kas konkreetse meetme puhul on tegemist kaudse nõudega andmete asukohale, siis tuleb võtta arvesse iga juhtumi eriomaseid asjaolusid.

Isikustamata andmete vaba liikumise määruses[38] osutatakse **avaliku julgeoleku** kontseptsioonile, nagu on kirjeldatud Euroopa Kohtu lahendites. Avalik julgeolek „hõlmab nii

---

33 Artikli 4 lõikes 1.

34 Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) artikli 3 punkt 5.

35 Pange tähele, et andmete asukoha nõuete seaduslikkuse ja ebaseaduslikkuse ulatusega seotud õiguskindlusetus piirab veelgi turuosaliste ja avaliku sektori võimalusi andmete töötlemise asukoha valimisel (vt Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) põhjendus 4).

36 Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) põhjendus 4.

37 Vt kaks uuringut andmete asukoha nõuete kohta, mis viidi läbi enne isikustamata andmete vaba liikumise määruse vastuvõtmist: (1) Godel, M. jt: *Facilitating cross border data flows in the Digital Single Market*, SMART nr 2015/2016; kättesaadav aadressil: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 ning (2) Time.lex, Spark Legal Network ja Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions.* SMART nr 2015/0054; kättesaadav aadressil: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

38 Põhjendus 19.

liikmesriigi sise- kui ka välisjulgeolekut[39] ning ühiskonna turvalisuse küsimusi, selleks, et eelkõige hõlbustada kuritegude uurimist, avastamist ja nende eest vastutusele võtmist. Selle puhul eeldatakse tõelise ja piisavalt tõsise ohu olemasolu, mis mõjutab ühte ühiskonna põhihuvi,[40] nagu oht institutsioonide ja oluliste avalike teenuste toimimisele ning elanike ellujäämisele, samuti välissuhete või rahvaste rahumeelse kooseksisteerimise tõsise häirimise oht või oht sõjalistele huvidele.“

Lisaks sellele peavad avaliku julgeoleku kaalutlustel põhjendatud andmete asukoha nõuded olema proportsionaalsed. Kooskõlas Euroopa Kohtu otsustega eeldab proportsionaalsuse põhimõte, et võetavad meetmed on sobilikud eesmärgi saavutamiseks ja ei lähe selleks vajalikust kaugemale.[41]

Selguse huvides olgu öeldud, et andmete asukoha nõuete keelamine ei piira juba ELi õigusega kehtestatud piiranguid[42].

Lisaks sellele ei kehtestata isikustamata andmete vaba liikumise määrusega kohustusi ettevõtjatele ega piirata nende lepingulist vabadust otsustada, kus nende andmeid töödeldakse.

Liikmesriigid peavad tegema nende territooriumil kohaldatavate andmete asukoha nõuete üksikasjad kättesaadavaks **liikmesriigi ühtses veebipõhises teabepunktis** (liikmesriigi veebisaidil). Nad peavad seda teavet ajakohastama või esitama ajakohastatud teabe liidu muu õigusakti alusel loodud kesksele teabepunktile[43]. Ettevõtjate mugavuse huvides ja et tagada sellele teabele lihtne juurdepääs kõikjal ELis, avaldab komisjon nende teabepunktide lingid portaalis Teie Euroopa[44].

---

39 Vt näiteks Euroopa Kohtu 23. novembri 2010. aasta otsus kohtuasjas Land Baden-Württemberg *vs*. Tsakouridis, C-145/09, ECLI:EU:C:2010:708, punkt 43 ning 4. aprilli 2017. aasta otsus kohtuasjas Sahar Fahimian *vs*. Saksamaa Liitvabariik, C-544/15, ECLI:EU:C:2017:225, punkt 39.

40 Vt näiteks Euroopa Kohtu 22. detsembri 2008. aasta otsus kohtuasjas Euroopa Ühenduste Komisjon vs. Austria Vabariik, C-161/07, ECLI:EU:C:2008:759, punkt 35 ja selles osutatud kohtulahendid ning 26. märtsi 2009. aasta otsus kohtuasjas Euroopa Ühenduste Komisjon *vs*. Itaalia Vabariik, C-326/07, ECLI:EC:C:2009:193, punkt 70 ja selles osutatud kohtulahendid.

41 Vt näiteks Euroopa Kohtu 8. juuli 2010. aasta otsus kohtuasjas Afton Chemical Limited *vs*. Secretary of State for Transport, C-343/09, ECLI:EU:C:2010:419, punkt 45 ja selles osutatud kohtulahendid.

42 Vt näiteks 28. novembri 2006. aasta direktiivi 2006/112/EÜ (mis käsitleb ühist käibemaksusüsteemi) artikli 245 lõige 2, milles on sätestatud, et „[l]iikmesriigid võivad nõuda, et nende territooriumil asuvad maksukohustuslased teataksid neile arvete säilitamiskoha juhul, kui see paikneb väljaspool nende territooriumi.“ Seda nõuet tuleb siiski lugeda koostoimes artikliga 249, milles on sätestatud, et „[k]ui maksukohustuslane säilitab enda väljastatud või saadud arveid elektroonilisel teel nii, et on tagatud *on-line* juurdepääs andmetele, ja kui säilituskoht paikneb muus liikmesriigis kui selles, kus ta asub, on tema asukohaliikmesriigi pädevatel asutustel käesoleva direktiivi kohaldamiseks õigus neile arvetele elektrooniliselt juurde pääseda, neid alla laadida ja neid kasutada maksukohustuslase asukohaliikmesriigi eeskirjade kohaselt ulatuses, mis on nendele asutustele vajalik järelevalveks.“

43 Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) artikli 4 lõige 4.

44 https://europa.eu/youreurope/index.htm

3.2. Isikuandmete vaba liikumine

Isikuandmete kaitse üldmääruses[45] on sätestatud, et „[i]sikuandmete vaba liikumist liidus ei piirata ega keelata põhjustel, mis on seotud füüsiliste isikute kaitsega isikuandmete töötlemisel.“

Kui liikmesriik kehtestab isikuandmete asukoha nõuded muul põhjusel kui isikuandmete kaitse, siis tuleb neid hinnata, võttes arvesse Euroopa Liidu toimimise lepingu[46,47] ning asjakohaste ELi õigusaktide (näiteks teenuste direktiiv[48] ja e-kaubanduse direktiiv[49]) sätteid põhivabaduste ja nendest vabadustest erandi tegemise lubatud põhjuste kohta.

Näide

Liikmesriigi õigusega nõutakse, et palgaandmed asuksid konkreetses liikmesriigis, näiteks liikmesriigi maksuhalduri tehtava regulatiivse kontrolli kaalutlustel. Liikmesriigi selline säte ei kuuluks isikuandmete kaitse üldmääruse artikli 1 lõike 3 kohaldamisalasse, kuna see põhjus ei ole seotud isikuandmete kaitsega. Selle asemel tuleks nõuet hinnata lähtuvalt Euroopa Liidu toimimise lepingu põhivabaduste sätetest ning nendest vabadustest erandite tegemise eeldustest.

Isikuandmete kaitse üldmääruses[50] tunnustatakse liikmesriikide õigust kehtestada tingimusi, sealhulgas piiranguid geneetiliste, biomeetriliste ja terviseandmete töötlemisele. Kuid nagu on märgitud põhjenduses 53, ei tohiks need liikmesriikide piirangud takistada isikuandmete vaba liikumist ELis, kui neid tingimusi kohaldatakse selliste andmete piiriülese töötlemise suhtes. See on kooskõlas Euroopa Liidu toimimise lepingu artikliga 16, milles sätestatakse isikuandmete kaitse õigust ja kõnealuste andmete vaba liikumist käsitlevate normide vastuvõtmise õiguslik alus.

[45] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) artikli 1 lõige 3.

[46] Euroopa Liidu toimimise lepingu konsolideeritud versioon (ELT C 326, 26.10.2012, lk 47–390.)

[47] Vt ka Euroopa Kohtu 19. juuni 2008. aasta otsus kohtuasjas Euroopa Ühenduste Komisjon *vs.* Luksemburgi Suurhertsogiriik, C-319/06, ECLI:EU:C:2008:350, punktid 90–91: kohtu hinnangul oli kohustus teha teatavad dokumendid kättesaadavaks ja neid säilitada teatavas liikmesriigis teenuste osutamise vabaduse piirang; põhjendus, et see hõlbustab üldiselt asutustel oma kontrolliülesannete täitmist, ei ole piisav.

[48] Euroopa Parlamendi ja nõukogu 12. detsembri 2006. aasta direktiiv 2006/123/EÜ teenuste kohta siseturul (ELT L 376, 27.12.2006, lk 36–68).

[49] Euroopa Parlamendi ja nõukogu 8. juuni 2000. aasta direktiiv 2000/31/EÜ infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (direktiiv elektroonilise kaubanduse kohta) (EÜT L 178, 17.7.2000, lk 1–16).

[50] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) artikli 9 lõige 4.

3.3. Isikustamata andmete vaba liikumise määruse kohaldamisala

Nagu juba eespool mainitud, on isikustamata andmete vaba liikumise määruse eesmärk tagada isikustamata andmete vaba liikumine liidus[51]. Seega ei kohaldata seda väljaspool ELi toimuva töötlemise ning kõnealuse töötlemisega seotud andmete asukoha nõuete suhtes[52,53].

Määruse kohaldamisala piirdub artikli 2 lõike 1 kohaselt seega elektrooniliste isikustamata andmete töötlemisega ELis:

(a) mille puhul on tegemist teenuse osutamisega kasutajatele, kelle elu- või tegevuskoht on ELis, sõltumata sellest, kas teenuseosutaja asukoht on ELis või mitte, või
(b) mida teeb oma tarbeks füüsiline või juriidiline isik, kelle elu- või tegevuskoht on ELis.

Näited

Isikustamata andmete vaba liikumise määruse artikli 2 lõike 1 punkt a:

- USAs asutatud pilvteenuse osutaja pakub oma teenuseid ELis elavatele või asutatud klientidele. Pilvteenuse osutaja haldab oma tegevust ELi territooriumil asuvate serverite abil, milles säilitatakse või töödeldakse muul viisil tema Euroopa klientide andmeid. Pilvteenuse osutaja ei pea omama taristut ELis, vaid võib ka näiteks rentida serveriruumi ELis. Selle andmetetöötluse suhtes kohaldatakse isikustamata andmete vaba liikumise määrust;
- Jaapanis asutatud pilvteenuse osutaja pakub oma teenuseid Euroopa klientidele. Teenuseosutaja töötlemisvõimsus paikneb Jaapanis ja kogu töötlemine toimub seal. Kui kogu töötlemine toimub väljaspool ELi, siis sel juhul isikustamata andmete vaba liikumise määrust ei kohaldata[54].

Isikustamata andmete vaba liikumise määruse artikli 2 lõike 1 punkt b:

- liikmesriigist A pärit väike Euroopa idufirma otsustab laiendada oma tegevust ja hakata tegutsema liikmesriigis B. Kulude minimeerimiseks otsustab see idufirma säilitada ja töödelda ka uue ettevõtte andmeid oma serveris, mis asub liikmesriigis A. Liikmesriigid

[51] Vt Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) artikkel 1.

[52] Vt Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) põhjendus 15.

[53] Töötlemise mõiste on määratletud üldsõnaliselt (Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) artikli 3 punkt 2) ning nagu on rõhutatud määruse põhjenduses 17 tuleks määrust kohaldada andmetöötluse suhtes selle kõige laiemas tähenduses, mis hõlmab mis tahes tüüpi IT-süsteemide kasutamist.

[54] Pange tähele, et Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määrus (EL) 2018/1807, mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku, ei reguleeri andmete asukoha nõudeid, mille liikmesriigid kehtestavad isikustamata andmete säilitamisele kolmandates riikides, ja need nõuded võivad olla kehtestatud liikmesriikide õigussüsteemides. Selguse huvides olgu märgitud, et isikuandmete kaitse üldmäärust kohaldatakse ELis asuvate andmesubjektide isikuandmete töötlemise suhtes, mille viib ellu vastutav või volitatud töötleja, kui töötlemine on seotud järgmisega: a) liidus asuvatele andmesubjektidele kaupade ja teenuste pakkumisega, olenemata sellest, kas andmesubjekt peab maksma tasu, või b) nende tegevuse jälgimisega, kui see tegevus toimub liidus (vt isikuandmete kaitse üldmääruse artikli 3 lõige 2).

ei tohi sellist IT tsentraliseerimist keelata, v.a kui see on põhjendatud avaliku julgeoleku kaalutlustel kooskõlas proportsionaalsuse põhimõttega.

Kuigi isikustamata andmete vaba liikumise määrust ei kohaldata juhul, kui isikustamata andmete kogu töötlemine toimub väljaspool ELi, tuleb isikuandmete kaitse üldmäärust järgida, kui andmekogu sisaldab isikuandmeid. Eelkõige tuleb igal juhul järgida isikuandmete kaitse üldmääruse norme, mis käsitlevad isikuandmete edastamist kolmandatele riikidele või rahvusvahelistele organisatsioonidele[55].

3.4. Liikmesriikide sisemise korraldusega seotud tegevus

Isikustamata andmete vaba liikumise määrus ei kohusta liikmesriike ostma sisse selliste isikustamata andmetega seotud teenuste osutamist, mida nad soovivad ise osutada või korraldada muul viisil kui riigihankelepingutena.[56]

Isikustamata andmete vaba liikumise määruse artikli 2 lõikes 3 on märgitud:

„Käesolev määrus ei piira õigus- ja haldusnorme, mis käsitlevad liikmesriikide **sisemist korraldust** ja millega nähakse ametiasutustele ja direktiivi 2014/24/EL artikli 2 lõike 1 punktis 4 määratletud avalik-õiguslikele isikutele[57] ette **andmete töötlemise** volitusi ja kohustusi **ilma eraõiguslike isikute lepingulise tasustamiseta** ning liikmesriikide õigus- ja haldusnorme, millega nähakse ette nende volituste ja kohustuste rakendamine.“[58]

Võib olla õigustatud huvisid, mille korral on põhjendatud osutada selliseid andmete töötlemise teenuseid ise, näiteks teenuste osutamine asutuse sees või avalike haldusasutuste vastastikused kokkulepped. Tavapärased näited on valitsuse pilve kasutamine või kui valitsus kasutab riigiasutustele ja -organitele andmete töötlemiste teenuste osutamiseks tsentraliseeritud IT-asutust.

---

[55] Lisateavet isikuandmete edastamise kohta kolmandatele riikidele leiate komisjoni veebilehelt https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_et ning *komisjoni teatisest Euroopa Parlamendile ja nõukogule „Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas“*, COM/2017/07 final, aadressil https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=COM:2017:7:FIN. Mis puudutab Jaapanit, siis komisjon võttis 23. jaanuaril 2019 vastu otsuse Jaapani kaitsetaseme piisavuse kohta, millega võimaldatakse isikuandmetel kahe majanduspiirkonna vahel vabalt liikuda tänu nende andmete kaitseks rakendatavatele tugevatele tagatistele.

[56] Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) põhjendus 14.

[57] Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiivi 2014/24/EL (riigihangete kohta ja direktiivi 2004/18/EÜ kehtetuks tunnistamise kohta (ELT L 94, 28.3.2014, lk 65–242)) artikli 2 lõike 1 punktis 4 on sätestatud, et „avalik-õiguslik isik“ on „isik, mis vastab kõigile järgmistele tingimustele: a) see on moodustatud konkreetse eesmärgiga rahuldada vajadusi üldistes huvides ning sellel ei ole tööstuslikku ega ärilist iseloomu; b) see on juriidiline isik ning c) seda rahastavad põhiliselt riik, piirkondlikud või kohalikud omavalitsused või muud avalik-õiguslikud isikud; selle juhtimine toimub kõnealuste omavalitsuste või avalik-õiguslike isikute järelevalve all; selle haldus-, juhtimis- või järelevalveorgani liikmetest üle poole on määranud riik, piirkondlik või kohalik omavalitsus või muud avalik-õiguslikud isikud.“

[58] Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) põhjenduse 13 kohaselt ei piira määrus direktiivi 2014/24/EL kohaldamist.

Kuid isikustamata andmete vaba liikumise määrus julgustab liikmesriike kaaluma asutusteväliste teenuseosutajate kasutamise majanduslikku tõhusust ja sellest saadavat muud kasu[59,60]. Niipea kui riigiasutused hakkavad korraldama andmete töötlemist allhanke korras, makstes eraõiguslikele isikutele lepingulist tasu, ning töötlemine toimub ELis, siis kohaldatakse selle töötlemise suhtes isikustamata andmete vaba liikumise määrust, mis tähendab, et riigiasutuste üldiste ja haldustavade suhtes kohaldatakse isikustamata andmete vaba liikumise põhimõtet. Eelkõige ei tohi nad kehtestada piiranguid andmete asukohale, näiteks riigihangete pakkumismenetlustes[61].

4. Iseregulatsioonil põhinevad lähenemisviisid, mis toetavad andmete vaba liikumist

Iseregulatsioon toetab innovatsiooni, suurendab turuosaliste vastastikust usaldust ja võimaldab turul toimuvatele muutustele paremini reageerida. Selles punktis esitatakse ülevaade iseregulatsiooni algatustest isiku- ja isikustamata andmete töötlemise valdkonnas.

4.1. Andmete portimine ja pilvteenuse osutajate vahetamine

Üks isikustamata andmete vaba liikumise määruse eesmärkidest on vältida seotuse tekitamist ühest teenuseosutajast. Seotus tekib juhul, kui kasutajad ei saa teenuseosutajat vahetada, kuna nende andmed on seotud ühte teenuseosutaja süsteemiga, näiteks konkreetse andmevormingu või lepingutingimuste tõttu, ning neid ei saa teenuseosutaja IT-süsteemist välja kanda. Ilma takistusteta andmete portimise võimalus on oluline, et kasutajad saaksid vabalt valida andmete töötlemise teenuse osutaja, ning seega oleks turul tagatud toimiv konkurents.

Ettevõtjatevaheline andmete porditavus muutub üha olulisemaks mitmes digitaaltööstuse valdkonnas, sh pilvteenuste puhul.

Isikustamata andmete vaba liikumise määruse artikli 6 kohaselt soodustab ja hõlbustab komisjon iseregulatsiooni tegevusjuhendite (edaspidi „tegevusjuhendid“) väljatöötamist ELi tasandil, et toetada konkurentsivõimelist andmepõhist majandust. Selle alusel saab tööstussektor töötada komisjoni toetusel välja iseregulatsiooni tegevusjuhendid, mis käsitlevad teenuseosutajate vahetamist ja andmete portimist eri IT-süsteemide vahel.

Andmete portimist käsitlevate tegevusjuhendite koostamisel tuleb võtta arvesse mitut aspekti, eelkõige:

- **parimaid tavasid**, mis lihtsustavad teenuseosutajate vahetamist ja andmete portimist struktureeritud, üldkasutatavas ja masinloetavas vormingus,

[59] Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) põhjendus 14.

[60] Asutuseväline teenuseosutaja oleks mis tahes üksus, mis ei ole avalik-õiguslik isik, nagu on sätestatud Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiivi 2014/24/EL (riigihangete kohta ja direktiivi 2004/18/EÜ kehtetuks tunnistamise kohta (ELTL 94, 28.3.2014, lk 65–242)) artikli 2 lõike 1 punktis 4.

[61] Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) põhjendus 13.

- **teabe esitamise miinimumnõudeid**, tagamaks et kutselistele kasutajatele esitatakse enne lepingu sõlmimist piisavalt üksikasjalikku ja selget teavet menetluse, tehniliste nõuete, ajakava ja kulude kohta, mida kohaldatakse juhul, kui kutseline kasutaja soovib teenuseosutajat vahetada, või andmete tagasi oma IT-süsteemidesse portimise kohta,
- **seda, kuidas lähenetakse sertifitseerimissüsteemidele** tänu millele on pilvteenuseid lihtsam võrrelda, ning
- **teabevahetuse tegevuskavasid**, mille abil suurendatakse teadlikkust tegevusjuhenditest.

Pilvteenuste turul on komisjon hakanud edendama digitaalse ühtse turu pilvteenuse sidusrühmadest koosnevate töörühmade tegevust, kuhu on koondunud pilvteenuste eksperdid ja kutselised kasutajad, sh väikesed ja keskmise suurusega ettevõtjad. Praegu töötab üks allrühm (SWIPO töörühm) [62] välja andmete portimise ja pilvteenuse osutajate vahetamise iseregulatsiooni tegevusjuhendeid ja teine allrühm (CSPCERTi töörühm)[63] töötab välja pilvteenuse turvalisuse sertifitseerimise süsteemi.

SWIPO töörühm töötab välja tegevusjuhendit, mis hõlmab kõiki pilvteenuste valdkondi: taristu teenusena (IaaS), platvorm teenusena (PaaS) ja tarkvara teenusena (SaaS).

Komisjon eeldab, et eri tegevusjuhendeid täiendatakse **lepingute näidistingimustega**[64]. Need võimaldavad tegelikkuses kasutamisel piisavat tehnilist ja õiguslikku konkreetsust ning tegevusjuhendite kohaldamist, mis on eriti oluline väikeste ja keskmise suurusega ettevõtjate jaoks. Lepingute näidistingimused on kavas koostada pärast tegevusjuhendite koostamist (mis peaksid valmima 29. novembriks 2019).

Isikustamata andmete vaba liikumise määruse artikli 8 kohaselt hindab komisjon määruse rakendamist 29. novembriks 2022. See võimaldab hinnata: i) andmete vaba liikumise mõju Euroopas, ii) määruse kohaldamist, eelkõige segaandmekogude suhtes, iii) seda, millises ulatuses on liikmesriigid tegelikult kaotanud kehtivad põhjendamatud andmete asukoha piirangud, ning iv) andmete portimist ja pilvteenuse osutajate vahetamist käsitlevate tegevusjuhendite mõju turgudele.

Porditavuse mõiste ja koosmõju isikuandmete kaitse üldmäärusega

Mõlemad määrused[65] osutavad andmete porditavusele ja eesmärgile lihtsustada andmete portimist ühest IT-keskkonnast teise, s.o teise teenuseosutaja süsteemidesse või kohapealsetesse süsteemidesse. See aitab vältida seotust ühe teenuseosutajaga ja soodustab teenuseosutajatevahelist konkurentsi. Kuid määrustes kasutatud portatiivsuse käsitlused erinevad sihthuvirühmade vahelise suhte ja sätete õigusliku olemuse osas.

62 Pilvteenuse osutajate vahetamise ja andmete portimise töörühm.

63 Euroopa pilvteenuseosutajate sertifitseerimise töörühm. Vt ka punkt 4.3.

64 Vt Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) põhjendus 30.

65 Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) artikkel 6 ning Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) artikkel 20.

Isikuandmete kaitse üldmääruse artiklis 20 sätestatud andmete ülekandmise õigus keskendub andmesubjekti ja vastutava töötleja vahelisele suhtele. See käsitleb andmesubjekti õigust saada isikuandmeid, mille ta on vastutavale töötlejale esitanud, struktureeritud ja üldkasutatavas vormingus ning masinloetaval kujul ning õigust edastada need andmed teisele vastutavale töötlejale või hakata neid ise säilitama, ilma et vastutav töötleja, kellele kõnealused isikuandmed on esitatud, seda takistaks[66]. Üldjuhul on selles suhtes olevad andmesubjektid eri veebiteenuste tarbijad, kes soovivad vahetada teenuseosutajat.

Isikustamata andmete vaba liikumise määruse artikliga 6 ei sätestata kutseliste kasutajate õigust andmeid portida, vaid sealne lähenemisviis põhineb iseregulatsioonil, millega kaasnevad tööstussektori vabatahtlikud tegevusjuhendid. Samal ajal käsitleb see olukorda, mille puhul kutseline kasutaja on tellinud oma andmete töötlemise kolmandast isikust andmetöötlusteenuse pakkujalt[67]. Isikustamata andmete vaba liikumise määruse artikli 3 punkti 8 kohaselt võib „kutseline kasutaja“ olla „füüsiline või juriidiline isik, sealhulgas ametiasutus või avalik-õiguslik isik, kes kasutab või taotleb andmetöötlusteenust oma kaubanduse, äri, kutseala, elukutse või ülesandega seotud eesmärkidel.“

Tegelikkuses on isikustamata andmete vaba liikumise määruse artiklis 6 käsitletud portatiivsus seotud ettevõtjatevaheliste suhetega kutselise kasutaja (kes võib juhul, kui töödeldakse ka isikuandmeid, olla vastutav töötleja isikuandmete kaitse üldmääruse tähenduses) ning teenuseosutaja (kes võib samal moel olla teatavatel juhtudel volitatud töötleja) vahel.

Hoolimata erinevustest võib segaandmekogude puhul tekkida olukordi, kui andmete portimise suhtes kohaldatakse nii isikustamata andmete vaba liikumise määrust kui ka isikuandmete kaitse üldmäärust.

Näide

Pilvteenust kasutav ettevõtja otsustab vahetada pilvteenuse osutajat ja portida kõik andmed uue teenuseosutaja süsteemi. Teenuseosutaja vahetamise ja andmete portimise suhtes kohaldatakse kliendi ja pilvteenuse osutaja sõlmitud lepingut. Kui eelmine pilvteenuse osutaja järgib isikustamata andmete vaba liikumise määruse alusel koostatud käitumisjuhendit, siis tuleb andmed portida kooskõlas seal sätestatud nõuetega.

[66] Vt artikli 29 töörühma *suunised andmete ülekandmise õiguse kohta*. WP 242 rev.01, vastu võetud 13. detsembril 2016, viimati muudetud ja vastu võetud 5. aprillil 2017.

[67] Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määruse (EL) 2018/1807 (mis käsitleb isikustamata andmete Euroopa Liidus vaba liikumise raamistikku) põhjenduses 29 on märgitud: „Kui üksiktarbijatele on kehtiv liidu õigus [s.o isikuandmete kaitse üldmäärus] kasulik, siis äris ja kutsealases tegevuses ei ole kasutajatel teenuseosutajate vahetamine lihtne.“

Kui porditud andmekogud sisaldavad ka isikuandmeid, siis tuleb portimisel järgida isikuandmete kaitse üldmääruse kõiki asjakohaseid sätteid, eelkõige tagada, et uus pilvteenuse osutaja järgib kohaldatavaid nõudeid, sealhulgas turvanõudeid[68].

Näide

Kui pank otsustab vahetada oma kliendisuhete haldamise (CRM) teenuseosutajat, siis on võimalik, et teatavad (isiku- ja isikustamata) andmed tuleb kanda eelmise teenuseosutaja süsteemist uue teenuseosutaja süsteemi. Nende andmete suhtes kohaldatakse sel juhul eri regulatiivseid nõudeid, millest mõned tulenevad isikuandmete kaitse üldmäärusest ja mõned isikustamata andmete vaba liikumise määrusest.

4.2. Isikuandmete kaitse tegevusjuhendid ja sertifitseerimissüsteemid

Isikuandmete kaitse üldmäärusest (vt artikli 24 lõige 3 ja artikli 28 lõige 5) tulenevate kohustuste täitmise tõendamiseks võib kasutada tegevusjuhendeid ja sertifitseerimissüsteeme.

Isikuandmete kaitse üldmääruse artikli 40 lõike 1 ja artikli 42 lõike 1 kohaselt peaksid liikmesriigid, järelevalveasutused, Euroopa Andmekaitsenõukogu ja komisjon julgustama tööstussektorit koostama tegevusjuhendeid ja võtma kasutusel andmekaitse sertifitseerimise mehhanisme.

Vastutavate või volitatud töötlejate konkreetset kategooriat esindavad ühendused või muud organid võivad koostada konkreetse sektori tegevusjuhendi. Tegevusjuhendi kavand tuleb esitada kinnitamiseks vastavale pädevale järelevalveasutusele[69]. Kui tegevusjuhendi kavand mõjutab andmete töötlemist mitmes liikmesriigis, siis peab järelevalveasutus esitama selle enne kinnitamist Euroopa Andmekaitsenõukogule. Euroopa Andmekaitsenõukogu esitab seejärel oma arvamuse selle kohta, kas tegevusjuhendi kavand vastab isikuandmete kaitse üldmäärusele.

Euroopa Andmekaitsenõukogu avaldas oma suunised 1/2019 isikuandmete kaitse üldmääruse kohaste tegevusjuhendite ja järelevalvet teostavate asutuste kohta[70]. Suunised sisaldavad teavet tegevusjuhendite koostamise ja nende kinnitamise kriteeriumide kohta ning muud kasulikku teavet. Samal moel annavad Euroopa Andmekaitsenõukogu suunised 1/2018 isikuandmete kaitse üldmääruse artiklite 42 ja 43 kohaselt sertifitseerimiskriteeriumide

[68] Vt artikli 29 töörühma *arvamus 05/2012 pilvandmetöötluse kohta*, mis võeti vastu 1. juulil 2012, WP196, milles täpsustatakse pilvteenuse kasutajate ja pilvteenuse osutajate seisundit ja kohustusi isikuandmete töötlemisel.

[69] Vt Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) artikli 40 lõige 5 ja artikkel 55.

[70] Euroopa Andmekaitsenõukogu: *suunised 1/2019 määruse 2016/679 kohaste tegevusjuhendite ja järelevalvet teostavate asutuste kohta*, vastu võetud 12. veebruaril 2019, avalikuks konsultatsiooniks mõeldud tekst on internetis kättesaadav aadressil: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_et

kindlaksmääramise ja sertifitseerimise kohta teavet kõnealuse määruse alusel sertifitseerimise, sertifitseerimiskriteeriumide väljatöötamise ja kinnitamise kohta[71].

Pilvteenuste tööstussektori koostatud tegevusjuhendite näited

ELi pilvteenuse tegevusjuhend koostati komisjoni toetusel koostöös pilvandmetöötluse töörühmaga Cloud Select Industry Group (C-SIG), lähtudes andmekaitsedirektiivist[72] ja seejärel isikuandmete kaitse üldmäärusest. ELi pilvteenuse tegevusjuhend hõlmab pilvteenuste kõiki aspekte: tarkvara teenusena (SaaS), platvorm teenusena (PaaS) ja taristu teenusena (IaaS)[73].

Euroopa pilvtaristu teenuseosutajate tegevusjuhend (CISPE)[74] keskendub IaaSi teenuse osutajatele. CISPE tegevusjuhend sisaldab nõudeid IaaSi teenuse osutajatele, kes tegutsevad andmete volitatud töötlejatena isikuandmete kaitse üldmääruse kohaselt. Sellega kehtestatakse ka nõuded juhtimisstruktuurile tegevusjuhendi rakendamiseks ja kohaldamiseks.

Cloud Security Alliance'i (CSA) tegevusjuhend isikuandmete kaitse üldmääruse järgimiseks on mõeldud kõigile pilvandmetöötlusest ja Euroopa isikuandmete õigusaktidest huvitatud sidusrühmadele, näiteks pilvteenuse osutajatele, pilvteenuse klientidele ja potentsiaalsetele klientidele, pilveaudiitoritele ja pilvtöötluse maakleritele. Tegevusjuhend käsitleb kõiki pilvteenuse osutajaid[75].

4.3. Usalduse suurendamine piiriülese andmetöötluse vastu – turvalisuse sertifitseerimine

Nagu on märgitud isikustamata andmete vaba liikumise määruse põhjenduses 33, peaks usalduse suurendamine andmete turvalise piiriülese töötlemise vastu vähendama turuosaliste ja avaliku sektori kalduvust kasutada andmete asukohta andmete turvalisuse tagatisena. Lisaks küberturvalisuse paketile, mille ettepaneku tegi komisjon 2017. aastal[76], koostab CSPCERT töörühm soovitusi Euroopa pilvteenuse sertifitseerimissüsteemi loomiseks, mis esitatakse komisjonile. See süsteem võib lihtsustada andmete vaba liikumist, võimaldada pilvteenuseid paremini võrrelda ja suurendada nende kasutuselevõttu. Komisjon võib esitada Euroopa Liidu Küberturvalisuse Ametile (ENISA) taotluse, et ta valmistaks ette kandidaatsüsteemi kooskõlas küberturvalisuse määruse asjakohaste sätetega[77]. See süsteem võib käsitleda nii isiku- kui ka isikustamata andmeid. Nagu märgitud punktis 4.2, võib andmete turvalisuse

[71] Euroopa Andmekaitsenõukogu: *suunised 1/2018 määruse 2016/679 artiklite 42 ja 43 kohaselt sertifitseerimiskriteeriumide kindlaksmääramise ja sertifitseerimise kohta*, vastu võetud 23. jaanuaril 2019, internetis kättesaadav aadressil: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_et

[72] Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (kaotas kehtivuse 24. mail 2018).

[73] Lisateavet ELi pilvteenuse tegevusjuhendi kohta leiate aadressil: https://eucoc.cloud/en/home.html

[74] Lisateavet CISPE tegevusjuhendi kohta leiate aadressil: https://cispe.cloud/code-of-conduct/

[75] Lisateavet CSA tegevusjuhendi kohta leiate aadressil: https://gdpr.cloudsecurityalliance.org/

[76] Lisateavet leiate aadressil https://ec.europa.eu/digital-single-market/en/cyber-security

[77] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus).

nõuetekohaste kaitsemeetmete olemasolu tõendamisel toetuda lisaks küberturvalisust käsitlevale õigusaktile ka isikuandmete kaitse üldmäärusele[78].

Lõppmärkused

Andmete töötlemisega seotud õiguskindlus ja usaldus on ülioluline, et EL saaks kasutada andmete kõiki võimalusi ka siis, kui väärtusahelad on sektori- ja piiriülesed. See tagatakse nende kahe määrusega, mille mõlema eesmärk on tagada andmete vaba liikumine. Isikustamata andmete vaba liikumise määrus ja isikuandmete kaitse üldmäärus koos loovad aluse andmete vabaks liikumiseks Euroopa Liidus ja väga konkurentsivõimelise Euroopa andmepõhise majanduse jaoks.

[78] Vt küberturvalisust käsitleva õigusakti põhjendus 74.