EUROOPA
KOMISJON

Brüssel, 24.7.2019
COM(2019) 374 final

KOMISJONI TEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE

Andmekaitse-eeskirjad kui usalduse tagajad ELis ja väljaspool – ülevaade

Komisjoni teatis Euroopa Parlamendile ja nõukogule

Andmekaitse-eeskirjad kui usalduse tagajad ELis ja väljaspool – ülevaade

I. Sissejuhatus

Isikuandmete kaitse üldmäärust[1] (edaspidi „määrus“) on Euroopa Liidus kohaldatud juba üle aasta. See on kõige olulisem osa ELi sidusast ja tänapäevasest andmekaitsemaastikust, kuhu kuuluvad veel õiguskaitse andmekaitse direktiiv[2] ning ELi institutsioonide ja organite andmekaitse direktiiv[3]. Kõnealusesse õigusraamistikku hakkab kuuluma ka koostamisel olev internetiprivaatsuse määrus.

Tugevad andmekaitse-eeskirjad on vajalikud isikuandmete kaitseks, mis on üks põhiõigustest. Need on demokraatliku ühiskonna jaoks keskse tähtsusega[4] ja üha enam andmetel põhineva majanduse oluline osa. EL püüab haarata kinni neist paljudest võimalustest, mida digitaliseerimine pakub teenuste, töökohtade ja innovatsiooni valdkonnas, aga tegeleda ühtlasi ka nendega kaasnevate probleemidega. Identiteedivargus, tundlike andmete lekked, diskrimineerimine, sisseehitatud kallutatus, ebaseadusliku sisu jagamine ja privaatsust rikkuvate jälgimisvõimaluste loomine on vaid mõni näide probleemidest, mis tulevad üha sagedamini jutuks avalikus mõttevahetuses, kust ilmneb selgelt, et inimesed eeldavad, et nende andmed on kaitstud.

Andmekaitsest on saanud tõeliselt üleilmne nähtus, sest kogu maailma inimesed hindavad ja väärtustavad üha enam oma andmete kaitset ja turvalisust. Paljud riigid on juba võtnud või võtmas vastu kõikehõlmavaid andmekaitse-eeskirju, mille aluseks on määruses sätestatutega sarnased põhimõtted ning mille tulemusel muutuvad andmekaitse-eeskirjad kogu maailmas ühesugusemaks. See pakub uusi võimalusi ettevõtete ja avaliku sektori asutuste andmeedastuse lihtsustamiseks ja parandab ühtlasi isikuandmete kaitset nii ELis kui ka kogu maailmas.

---

[1] 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): https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679.

[2] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta 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): https://eur-lex.europa.eu/legal-content/ET/ALL/?uri=celex:32016L0680. Liikmesriigid pidid direktiivi riigisisesesse õigusesse üle võtma 6. maiks 2018. Ülevõtmise seisu kohta saab ülevaate julgeolekuliidu aruannetest.

[3] 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 39–98): https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32018R1725. Kohaldatakse alates 11. detsembrist 2018.

[4] India ülemkohus tunnistas privaatsuse 24. augustil 2017 langetatud märgilise tähtsusega otsuses põhiõiguseks, märkides, et see on inimväärikuse oluline osa.

Andmekaitsesse suhtutakse üha tõsisemalt ning sel on eri sidusrühmadele ja sektoritele laialdane mõju. Komisjon on kindlalt otsustanud olla ELis uue andmekaitsekorra rakendamise eestvedaja ja aidata sel igati korralikult toimima hakata. Käesoleva teatisega annab komisjon ülevaate seni saavutatud tulemustest: kui järjepidevalt on andmekaitse-eeskirju ELis rakendatud, kuidas toimib uus juhtimissüsteem, milline on olnud mõju kodanikele ja ettevõtetele ning mida on eri riikide andmekaitsekorra üldisel lähendamisel teinud EL. Teatises vaadeldakse, mis on muutunud pärast 2018. jaanuaris määruse kohaldamise kohta avaldatud teatist[5], ning selles on arvesse võetud määruse sidusrühmade töörühma[6] tööd, eriti selle panust aasta möödumisel tehtud kokkuvõtetesse, ja komisjoni korraldatud ülevaateüritusel 13. juunil 2019. aastal toimunud arutelusid[7]. Käesolev teatis on aluseks ka läbivaatamisele, mis on kavandatud 2020. aasta maisse.[8]

ELi andmekaitse õigusraamistik on Euroopa inimkeskse innovatsiooni nurgakivi. Regulatiivse aluse ühe osana kasutatakse seda üha enamates poliitikavaldkondades, nagu tervishoid, teadus, tehisintellekt, transport, energeetika, konkurents ja õiguskaitse. Komisjon on järjekindlalt rõhutanud, kui tähtis on uute andmekaitse-eeskirjade korralik rakendamine ja jõustamine, nagu on esile toodud ka 2018. aasta jaanuari teatises määruse rakendamise kohta ja 2018. aasta septembris avaldatud komisjoni juhistes isikuandmete kasutamise kohta valimiste kontekstis[9]. Käesoleva teatise koostamise ajal on selle eesmärgi saavutamiseks juba palju ära tehtud, aga et määrus täiel määral toimima hakkaks, on kindlasti vaja veel palju tööd.

II. Üks maailmajagu, ühed eeskirjad: andmekaitseraamistik on liikmesriikides paigas

Määruse üks peamisi eesmärke oli kaotada varasema andmekaitsedirektiivi[10] alusel kehtestatud killustunud õigusaktid, mis olid kõigis 28 riigis erinevad, ning anda inimestele ja ettevõtetele kogu liidus õiguskindlus. See on enamjaolt saavutatud.

---

5 Komisjoni teatis Euroopa Parlamendile ja nõukogule „Parem kaitse ja uued võimalused – komisjoni suunised isikuandmete kaitse üldmääruse vahetu kohaldamise kohta alates 25. maist 2018“ (COM(2018) 43 final): https://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

6 Määruse sidusrühmade töörühm, mille on loonud komisjon ning milles osalevad kodanikuühiskonna ja ettevõtete esindajad, teadlased ning praktikud: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.

7 http://europa.eu/rapid/press-release_IP-19-2956_et.htm.

8 Määruse artikkel 97.

9 Komisjoni juhised liidu andmekaitseõiguse kohaldamise kohta valimiste kontekstis (COM(2018) 638 final): https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52018DC0638&qid=1566506566548&from=EN.

10 Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex:31995L0046.

Õigusraamistiku ühtlustamine

Kuigi määrus on liikmesriikides otsekohalduv, on selles neile pandud kohustus võtta riigi tasandil mitu õiguslikku meedet, täpsemalt asutada riiklikud andmekaitseasutused ja anda neile volitused[11], kehtestada eeskirjad teatavate probleemküsimuste jaoks (isikuandmete kaitse ning väljendus- ja teabevabaduse ühildamine) ning muuta andmekaitsenorme sisaldavaid valdkondlikke õigusakte (või need tühistada). Teatise koostamise ajaks olid kõik liikmesriigid (v.a kolm[12]) oma riigisisesed andmekaitsenormid ajakohastanud. Valdkondlike õigusaktide ajakohastamine veel käib. Pärast määruse inkorporeerimist Euroopa Majanduspiirkonna lepingusse laienes selle kohaldamine ka Norrasse, Islandile ja Liechtensteini, kes on samuti vastu võtnud oma riigisisesed andmekaitsenormid.

Sidusrühmad nõuavad aga kohati veelgi suuremat ühtlustamist.[13] Määrusega lubatakse liikmesriikidel tõesti veidi täpsustada selle kohaldamist teatavates valdkondades (nt iga, millest alates võivad lapsed hakata internetipõhiseid teenuseid kasutama vanema loata[14], või isikuandmete töötlemine valdkondades, nagu meditsiin ja tervishoid). Sellisel juhul peavad aga liikmesriigid arvesse võtma kahte aspekti:

i) kõik täpsustavad riigisisesed normid peavad olema kooskõlas põhiõiguste harta nõuetega[15] (ning mitte väljuma määruse kui hartal põhineva õigusakti kehtestatud piiridest);
ii) need ei tohi takistada isikuandmete vaba liikumist liidus.[16]

Mõnel juhul on liikmesriik kehtestanud määruses sätestatutele lisaks ka riigisisesed nõuded, eriti valdkondlikes õigusaktides, ning see tekitab killustatust ja ebavajalikku lisatööd. Üks näide sellisest lisanõudest on Saksamaa kehtestatud kohustus, et vähemalt 20 töötajaga ettevõtetes, kes tegelevad alaliselt isikuandmete automatiseeritud töötlemisega, peab olema andmekaitseametnik.

Jätkuv töö suurema ühtlustatuse nimel

Komisjon on riikide ametiasutustega pidevas kahepoolses dialoogis, pöörates erilist tähelepanu alljärgnevaga seotud riigisisestele meetmetele:

- andmekaitseasutuste reaalne sõltumatus (sh piisavate rahaliste, inim- ja tehniliste ressursside tagatus);
- andmesubjektide õiguste piirangud riigisisestes õigusaktides;

---

11 Nt haldustrahvi tegemise volitused.
12 23. juuli 2019. aasta seisuga on Kreekal, Portugalil ja Sloveenial nende vastuvõtmine veel pooleli.
13 Vt määruse sidusrühmade töörühma 13. juuni 2019. aasta aruanne: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.
14 Belgias, Eestis, Lätis, Maltal, Rootsis, Soomes, Taanis ja Ühendkuningriigis on see vanus 13 aastat; Austrias, Bulgaarias, Hispaanias, Itaalias, Küprosel ja Leedus 14; Prantsusmaal ja Tšehhis 15 ning Horvaatias, Iirimaal, Luksemburgis, Madalmaades, Poolas, Rumeenias, Saksamaal, Slovakkias ja Ungaris 16.
15 Artikkel 8.
16 Kooskõlas Euroopa Liidu toimimise lepingu artikli 16 lõikega 2.

- riigisiseses õiguses ei tohiks kehtestada määruses sätestatutest rangemaid nõudeid valdkondades, kus täpsustamisvõimalust pole (nt lisanõuded töötlemisele);
- kas on täidetud nõue ühildada isikuandmete kaitse ning väljendus- ja teabevabadus, arvestades et selle nõude väärkasutamisega ei tohi avaldada ajakirjandusele heidutavat mõju.

Andmekaitseasutuste koostöö Euroopa Andmekaitsenõukogus (edaspidi „andmekaitsenõukogu“) on peamine uute eeskirjade järjepideva kohaldamise tagaja: mitut liikmesriiki puudutavad täitmise tagamise meetmed läbivad andmekaitsenõukogus koostöö ja järjepidevuse tagamise süsteemi[17] ning nõukogu suunised aitavad kaasa määruse ühtsele tõlgendamisele. Sidusrühmad ootavad andmekaitseasutustelt siiski enamat.

Andmekaitse-eeskirjade tõlgendamise järjepidevust aitavad tagada ka riikide kohtud ja Euroopa Liidu Kohus. Riikide kohtud on hiljuti teinud otsuseid, millega tunnistatakse määruses sätestatust lahknevad riikliku õiguse sätted õigustühiseks.[18]

III. Uue juhtimissüsteemi kõik osad saavad järk-järgult paika

Määrusega loodi uus juhtimisstruktuur, milles on kesksel kohal riiklikud sõltumatud andmekaitseasutused, kes tegelevad määruse täitmise tagamisega ja toimivad sidusrühmade jaoks esmaste kontaktpunktidena. Kuigi enamik andmekaitseasutustest on viimasel aastal saanud ressursse juurde, on liikmesriikide vahelised erinevused endiselt suured.[19]

Andmekaitseasutused kasutavad oma uusi volitusi

Määrus annab andmekaitseasutustele suuremad täitmise tagamise volitused. Kuigi mõned sidusrühmad kartsid enne 2018. aasta maid vastupidist, on riiklikud andmekaitseasutused kasutanud oma täitmise tagamise volitusi tasakaalustatult. Sanktsioonide asemel on kasutatud pigem dialoogi, eriti väikeettevõtete puhul, kelle jaoks ei ole isikuandmete töötlemine põhitegevus. Siiski ei kardetud vajaduse korral oma uusi volitusi ka tegelikult käiku lasta, alustades uurimist sotsiaalmeedia valdkonnas[20] või kohaldades olenevalt rikkumise raskusastmest ka haldustrahve alates mõnest tuhandest kuni mitme miljoni euroni.

Näiteid andmekaitseasutuste kohaldatud trahvidest[21]:

- 5 000 eurot Austria spordikihlvedude kohvikule ebaseadusliku videovalve eest;

---

17 Määruse artiklis 60 on sätestatud andmekaitseasutuste koostöö selle nimel, et määrust tõlgendataks konkreetsetel juhtudel ühetaoliselt. Artikli 64 kohaselt annab andmekaitsenõukogu teatavatel juhtudel välja arvamusi, mis peaksid tagama määruse järjepideva kohaldamise. Samuti on andmekaitsenõukogul õigus teha siduvaid otsuseid juhtudel, kui andmekaitseasutused ei suuda saavutada üksmeelt.

18 Nii on juhtunud Hispaanias ja Saksamaal.

19 https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

20 Näiteks Iiri andmekaitsekomisjon alustas hargmaiste tehnoloogiaettevõtete suhtes määrusega seoses 15 ametlikku uurimist. Vt Iiri andmekaitsekomisjoni 2018. aasta aruande lk 49: https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018.

21 Mitu trahviotsust on edasi kaevatud.

- 220 000 eurot Poola andmevahendusettevõttele andmesubjektide teavitamata jätmise eest;
- 250 000 eurot Hispaania jalgpalliliigale LaLiga nutitelefoni rakenduse läbipaistmatuse eest;
- 50 miljonit eurot Google'ile Prantsusmaal kasutajatelt nõusoleku küsimise tingimustega seotud rikkumise eest.

Uurimisel peavad andmekaitseasutused kindlasti koguma asjassepuutuvat tõendusmaterjali, järgima kohalike õigusaktide kohast tegevuskorda ja tagama sageli keeruliste toimikute nõuetekohase menetluse. See nõuab aega ja märkimisväärselt palju tööd, mis selgitab ka seda, miks enamik pärast määruse kohaldamise algust algatatud uurimistest on veel pooleli.

Sellegipoolest tuleks määruse edu mõõta mitte kohaldatud trahvide arvuga, vaid kõigi asjaosaliste käitumise muutumisega. Andmekaitseasutustel on selles kontekstis teisigi meetodeid, nagu näiteks ajutise või alalise töötluskeelu kohaldamine (sh kolmandas riigis asuvale saajale andmete edastamise peatamine või keelamine).[22]

Mõned andmekaitseasutused on loonud uusi abivahendeid (nt abiliinid ja -materjalid ettevõtetele) või uuenduslikke meetmeid (nt isikuandmeid sisaldavate uuenduslike toodete ja teenuste arendamise regulatiivne katsetuskeskkond[23], mis aitab ettevõtetel määruse nõudeid täita). Mõned sidusrühmad tunnevad siiski, et pole saanud piisavalt tuge ja teavet (eriti mõne riigi VKEd).[24] Selle probleemi lahendamiseks annab komisjon andmekaitseasutustele nende sidusrühmadega (eriti üksikisikute ja VKEdega) tegelemiseks toetusi.[25]

Euroopa Andmekaitsenõukogu tegutseb

Andmekaitseasutused on hakanud Euroopa Andmekaitsenõukogu[26] töös aktiivsemalt kaasa lööma. Selle tulemusena on nõukogu võtnud määruse oluliste tahkude kohta vastu umbes 20 suunist[27]. Andmekaitsenõukogu tulevased töövaldkonnad on kirjas kahe aasta tööprogrammis[28] (nagu määruses nõutud).

---

22 Artikli 58 lõike 2 punktid f ja j.

23 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/.

24 Vt andmekaitse üldmääruse sidusrühmade töörühma aruanne: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

25 2018. aastal eraldati üheksa andmekaitseasutuse 2018.–2019. aasta meetmeteks 2 miljonit eurot: Belgiale, Bulgaariale, Islandile, Leedule, Lätile, Madalmaadele, Sloveeniale, Taanile ja Ungarile: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;
2019. aastal on kavas eraldada 1 miljon: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.

26 Euroopa Andmekaitsenõukogu on juriidiline isik ning sinna kuuluvad riiklike andmekaitseasutuste juhatajad ja Euroopa Andmekaitseinspektor.

27 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_et.

28 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_et.

Piiriüleste juhtumite puhul ei ole andmekaitseasutused enam lihtsalt riiklikud asutused, vaid osa tõeliselt üleeuroopalisest menetlusest: alates uurimisest kuni otsuse langetamiseni. Selline tihe koostöö on saanud igapäevaseks: 2019. aasta juuni lõpuks oli koostöösüsteemis tegeletud 516 piiriülese juhtumiga.

Komisjon aitab nõukogu tööle aktiivselt kaasa[29], et levitada teavet määruse sätte ja mõtte kohta, ning tuletab meelde ELi õiguse üldprintsiipe.[30]

ELi andmekaitsekultuuri loomine

Uue juhtimissüsteemi kogu potentsiaali ei ole veel kasutusse võetud. Andmekaitsenõukogu peab oma otsustusprotsessi veelgi sujuvamaks muutma ja kujundama oma liikmete seas välja ühise ELi andmekaitsekultuuri. Sellele aitab kaasa andmekaitseasutuste võimalus oma jõud mitut riiki hõlmavate probleemide korral koondada[31] (nt korraldada ühisuurimisi ja ühist täitmise tagamist), mis leevendab ka ressursikitsikust.

Paljud sidusrühmad tahavad näha veel rohkem koostööd ja riiklike andmekaitseasutuste ühtset tegutsemist.[32] Samuti soovivad nad suuremat järjepidevust andmekaitseasutuste antud nõuannetes[33] ja riigisiseste suuniste täielikku kooskõla andmekaitsenõukogu omadega. Mõned ootavad ka määruse põhimõistete (nt riskipõhine lähenemine) paremat selgitamist, võttes arvesse just VKEde murekohti.

Selleks on hädavajalik anda sidusrühmadele paremad võimalused anda tagasisidet andmekaitsenõukogu töö kohta. Sellepärast on komisjonil hea meel selle üle, et andmekaitsenõukogu konsulteerib suuniste üle süstemaatiliselt ka avalikkusega. Seda tava, nagu ka sidusrühmade tööseminaride korraldamist konkreetsete teemade arutamise algetapis, tuleks jätkata ja süvendada, et nõukogu töö oleks läbipaistev, kaasav ja asjakohane.

IV. Inimesed kasutavad oma õigusi, aga teadlikkust tuleks veelgi suurendada

Määruse teine tähtis eesmärk oli tugevdada inimeste õigusi. Enamik kodanikuõiguste ühendusi ja tarbijaorganisatsioone leiavad, et määrus aitab vastastikusel usaldusel põhineva õiglase digiühiskonna kujunemisele palju kaasa.

Parem teadlikkus andmekaitseõigustest

ELi inimesed on üha paremini teadlikud andmekaitse-eeskirjadest ja oma õigustest: Eurobaromeetri 2019. aasta mai küsitlusele[34] vastanutest 67% on määrusest teadlikud ning

---

29 Hääleõiguseta osalejana.

30 Komisjon on aidanud kaasa ka andmekaitsenõukogu asutamisele ja toetab selle toimimist oma kommunikatsioonisüsteemi kasutamise võimaldamisega.

31 Määruse artikkel 62.

32 Vt määruse sidusrühmade töörühma aruanne: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670. Näiteks arvavad ettevõtjad, et määruse artikli 35 kohast andmekaitsealast mõjuhinnangut nõudvate töötlemistoimingute riiklikud loetelud võiksid olla ühtlustatumad.

33 Sh eri liidumaade vms asutustelt saadud nõuannetes.

34 http://europa.eu/rapid/press-release_IP-19-2956_et.htm.

57% teavad, et on olemas riiklik andmekaitseasutus, kuhu nad võivad teabe küsimiseks ja kaebuste esitamiseks pöörduda. 73% olid kuulnud vähemalt ühest neile määrusega antud õigusest. Sellegipoolest ei võta väga paljud ELi inimesed internetis oma isikuandmete kaitsmiseks veel midagi ette. Näiteks 44% vastanutest kasutab sotsiaalvõrgustikke vaikevalikuna määratud privaatsusseadetega, ilma neid ise muutmata.

Inimesed kasutavad oma õigusi üha enam

Suurem teadlikkus oma õigustest on pannud inimesi neid ka rohkem kasutama: esitatakse klientidena päringuid, küsitakse andmekaitseasutustelt rohkem teavet või esitatakse neile kaebusi.[35] Ettevõtted annavad ka teada, et isikuandmetega tutvumise taotluste arv on suurenenud mitmes valdkonnas (nt panganduses ja telekommunikatsioonis). Samuti on inimesed üha enam keeldunud ärilistest teadaannetest või võtnud tagasi oma nõusoleku neid saada.[36]

Mõned ettevõtted on siiski teada andnud ka andmekaitse-eeskirjade vääritimõistmisest: mõnikord arvavad inimesed, et nad peavad nõustuma igasuguse andmetöötlusega või et õigus andmete kustutamisele on absoluutne (aga ettevõtted peavad isikuandmeid vahel säilitama juriidiliste kohustuste tõttu).[37] Teisalt kaebavad kodanikuühiskonna organisatsioonid, et mõni ettevõte või andmekaitseasutus viivitab vastamisega liiga kaua.

Oluline on, et valitsusvälised organisatsioonid on pärast kodanikelt volituste saamist esitanud mitu esindushagi, mida määrus nüüd võimaldab.[38] Esindushagide esitamine oleks olnud lihtsam, kui rohkem liikmesriike oleks kasutanud määruses antud võimalust lubada valitsusvälistel organisatsioonidel esitada hagi selleks volitusi küsimata.[39]

Teadlikkuse suurendamist on vaja jätkata

Seetõttu tuleb üldsuse teadlikkuse suurendamist ja dialoogi jätkata nii riiklikul kui ka ELi tasandil. Selleks käivitas komisjon 2019. aasta juulis uue veebikampaania[40], millega ärgitatakse inimesi privaatsusteateid lugema ja oma privaatsusseadeid optimeerima.

V. Ettevõtted kohandavad oma tavasid

Määruse eesmärk on toetada ettevõtteid digitaalmajanduses, pakkudes neile tulevikukindlaid lahendusi. Ettevõtetel on määruses sätestatud vastutuspõhimõtte üle üldiselt hea meel, sest see kaotab varasema koormava korra (kaob teavitusnõue, kohustuste suurus on kohandatav ning lõimitud ja vaikimisi andmekaitse põhimõte on paindlik, võimaldades konkurentsi privaatsust

---

35 https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.
36 Vt andmekaitse üldmääruse sidusrühmade töörühma aruanne.
37 Vt andmekaitse üldmääruse sidusrühmade töörühma aruanne.
38 Määruse artikli 80 lõige 1.
39 Määruse artikli 80 lõige 2.
40 See on järg eelmisele kampaaniale, mille käigus jagati inimestele ja ettevõtetele teabematerjale: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_et.

kaitsvate lahenduste põhjal). Mõned ettevõtted aga soovivad ka suuremat õiguskindlust ja rohkem või selgemaid suuniseid andmekaitseasutustelt.[41]

Usaldusväärne andmehaldus

Kuigi ettevõtted annavad teada paljudest probleemidest uute eeskirjadega kohanemisel,[42] rõhutavad paljud, et see oli hea võimalus juhtida ka ettevõtte juhatuse tähelepanu andmekaitsele, korrastada oma andmebaase, täiustada turvalisust, olla paremini valmis intsidentideks, vähendada tarbetuid riske ning tuua klientide ja äripartneritega suhtlemisse rohkem usaldust. Läbipaistvusega seoses mainivad ettevõtted ja kodanikuühiskonna organisatsioonid vajadust saavutada tasakaal määruse kohaselt inimestele antava teabe sisu ja vormi vahel, et see oleks inimestele arusaadav (selges ja lihtsas keeles ja vormingus). Ettevõtted arendavad selleks uuenduslikke lahendusi.

Üldiselt andsid ettevõtted teada, et suudavad andmesubjektide õigustega arvestada, kuigi sageli oli tähtaegadest kinnipidamine keeruline, sest taotlusi oli palju ja väga erinevaid,[43] ning probleeme tekitas ka taotluse esitajate isikusamasuse kontroll.

Mõju innovatsioonile

Määrus mitte ainult ei võimalda vaid lausa soodustab uue tehnoloogia väljatöötamist selliselt, et tagatud oleks ka põhiõigus isikuandmete kaitsele. Nii on see näiteks tehisintellekti valdkonnas.

Ettevõtted on hakanud pakkuma uusi, privaatsust paremini kaitsvaid teenuseid. Näiteks mõnes liikmesriigis kasvab jõudsalt selliste otsimootorite turuosa, mis ei jälgi kasutust ega kuva käitumispõhiseid reklaame. Mõned ettevõtted arendavad teenuseid, mille aluseks on inimestele antud uued õigused (nt andmete ülekantavus). Üha enam ettevõtteid kasutab isikuandmetega lugupidavat ümberkäimist konkurentsieelise ja müügiargumendina. Sellised muutused ei piirdu ELiga, vaid leiavad aset ka tugevalt uuenduslikes välisriikides.[44]

N-ö väikese riskiga mikro- ja väikeettevõtete olukord

Eri riikides on olukord küll erinev, aga mikro- ja väikeettevõtetel[45], kes ei töötle isikuandmeid oma põhitegevusena, on määruse kohaldamise kohta tavaliselt kõige rohkem küsimusi. Kuigi näib, et need on peamiselt tingitud andmekaitse-eeskirjade mittetundmisest, suurendavad nende muret vahel ka konsultatsioonibüroode kampaaniad, milles pakutakse tasulist

---

41 Vt määruse sidusrühmade töörühma aruanne.

42 IT-süsteemi ajakohastamist mainitakse sageli peamise probleemina, eriti seoses lõimitud ja vaikimisi andmekaitsega ning õigusega nõuda andmete kustutamist ka varukoopiatest jms.

43 Samuti soovivad ettevõtted, et andmekaitsenõukogu esitaks suunised põhjendamatute ja ülemääraste taotluste kohta.

44 Näiteks Iisraeli küberturvalisuse ettevõtete ühenduse 2018. aastal avaldatud aruande kohaselt oli andmekaitse ja privaatsus (osaliselt andmekaitse üldmääruse jõustumise tõttu) kõige kiiremini kasvav küberturvalisuse alamvaldkond.

45 Nagu on esitatud VKEde määratluses aadressil https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_et.

nõustamist, valeinfo levimine (nt et inimestelt tuleb süstemaatiliselt nõusolekut küsida[46]) ja riiklikul tasandil kehtestatud lisanõuded.

Seepärast soovivad mikro- ja väikeettevõtted just neile mõeldud ja väga praktilisi suuniseid. Mõned andmekaitseasutused on need juba riiklikul tasandil koostanud.[47] Riigisisestele algatustele lisaks on komisjon avaldanud teabematerjale, mis aitavad nendel ettevõtetel rea praktiliste nõuannete abil uusi eeskirju järgida.[48]

Määruses sätestatud abivahendite kasutamine

Määruses on sätestatud abivahendid, millega tõendada nõuetele vastavust: lepingu tüüptingimused, toimimisjuhendid ja uued sertifitseerimismehhanismid.

Lepingu tüüptingimused on näidissätted, mille võib vabatahtlikult lisada näiteks vastutava ja volitatud töötleja vahelisse lepingusse ning milles on kirjas lepinguosaliste määrusest tulenevad kohustused. Määruse järgi saab lepingu tüüptingimusi kasutada nii ELi sees kui ka väljaspool seda toimuvate andmeedastuste jaoks.[49] Just viimasel juhul kasutatakse neid laialdaselt,[50] mis näitab, et neist on ettevõtetele väga palju kasu, eriti siis, kui pole piisavalt ressursse, et pidada iga andmetöötlustöövõtjaga eraldi läbirääkimisi.

Mitu majandusharu peavad lepingu tüüptingimuste vastuvõtmist ühtlustamise seisukohalt väga kasulikuks, eriti kui vastuvõtja on komisjon. Komisjon kasutab koostöös sidusrühmadega määruse pakutud võimalusi ja ajakohastab olemasolevaid sätteid.

Toimimisjuhendite järgimine on teine praktiline ja kasulik abivahend, millega ettevõtted saavad määruse nõuete täitmist tõendada.[51] Toimimisjuhendid peaksid välja töötama valdkonna organisatsioonid või vastutavate ja volitatud töötlejate eri liike esindavad organisatsioonid ning neis tuleks kirjeldada andmekaitse eeskirjade rakendamist konkreetses valdkonnas. Kuna toimimisjuhendid aitavad kohustusi riskide alusel kohandada[52], on neist väga palju kasu VKEdele, kes saavad nii oma kohustusi täita kulutasuvamalt.

Kolmandana on määruse nõuete järgimise tõendamisel abi sertifitseerimisest. See aitab suurendada ettevõtete õiguskindlust ja edendada määruse nõuete järgimist kogu maailmas. ELis saab luua sertifitseerimissüsteeme Euroopa Andmekaitsenõukogu hiljuti vastuvõetud

---

46 Määruse kohaselt ei ole isikuandmete töötlemise õiguslikuks aluseks mitte ainult nõusolek, vaid mitu muudki põhjust.

47 Näiteks Prantsusmaa andmekaitseasutuse koostatud juhend: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement.

48 https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-et-n.pdf.

49 Vt määruse artikkel 28. Komisjoni vastu võetud lepingu tüüptingimused kehtivad kogu ELis. Seevastu tüüptingimused, mille on määruse artikli 28 lõike 8 kohaselt vastu võtnud riiklik andmekaitseasutus, on siduvad ainult sellele asutusele, nii et neid saab lepingu tüüptingimustena kasutada ainult nende töötlemistoimingute puhul, mis jäävad tema vastutusalasse (vt määruse artiklid 55 ja 56).

50 Tegelikult ongi need peamine abivahend, millele ettevõtted andmete teise riiki eksportimisel toetuvad.

51 Euroopa Andmekaitsenõukogu võttis toimimisjuhendite suunised vastu 4. juunil 2019. Neis on selgitatud toimimisjuhendite riiklikul ja ELi tasandil esitamise, heakskiitmise ja avaldamise korda.

52 Määruse põhjendus 98.

sertifitseerimis- ja akrediteerimissuuniste[53] alusel. Komisjon jälgib seda ja kasutab vajaduse korral määruses antud volitusi sertifitseerimisnõudeid täpsustada. Samuti võib komisjon esitada ELi standardiorganisatsioonidele teatavate määruse seisukohalt oluliste elementide standardimise taotluse.

VI. Nõuded ühtlustuvad ka rahvusvahelisel tasandil

Nõudmine isikuandmete kaitsmise järele ei piirdu vaid ELiga. Nagu selgus hiljutisest interneti turvalisuse uuringust, väheneb usaldus kogu maailmas ja see paneb inimesi veebis oma käitumist muutma.[54] Üha enam ettevõtteid lahendab seda probleemi nii, et laiendab määruses sätestatud õigusi ka ELi-välistele klientidele.

Kuna kogu maailmas esineb üha enam sarnaseid probleeme, võtavad paljud riigid vastu uusi andmekaitse-eeskirju või ajakohastavad olemasolevaid. Neis on palju liidu andmekaitsekorraga sarnast: üldised õigusnormid valdkondlike asemel, jõustatavad individuaalsed õigused ja sõltumatu järelevalveasutus. See suundumus on tõepoolest üleilmne ning esineb Lõuna-Koreast Brasiiliani, Tšiilist Taini ja Indiast Indoneesiani. Teine selge märk nõuete ühtlustumisest on Euroopa Nõukogu konventsiooniga nr 108[55] (mille hiljutisse ajakohastamisse andis olulise panuse ka komisjon[56]) ühinenud riikide arvu kasv kogu maailmas.

Andmete turvalise aga vaba liikumise edendamine kaitse piisavuse otsuste ja muuga

Nõuete ühtlustamine pakub uusi võimalusi andmete edastamises ning seetõttu ka äris ja riigiasutuste koostöös, täiustades sealjuures ELi kodanike andmete kaitset nende välismaale saatmisel.

---

53 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_et; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_et.

54 Vt 2019 CIGI-Ipsos Global Survey on Internet Security and Trust *[Rahvusvahelise juhtimisinnovatsiooni keskuse ja uuringufirma Ipsos 2019. aasta üleilmne interneti turvalisuse ja usalduse uuring]*. Uuringu kohaselt tundis 78% vastanutest muret oma privaatsuse pärast internetis; 49% ütlesid, et usaldamatuse tõttu avaldasid nad veebis vähem isikuandmeid; 43% ütlesid, et hoolitsevad varasemast rohkem oma seadmete turvalisuse eest, ning 39% vastas, et kasutavad internetti muudele ennetusmeetmetele lisaks ka valivamalt. Uuring korraldati 25 riigis: Ameerika Ühendriikides, Austraalias, Brasiilias, Egiptuses, Hiinas, Hongkongis, Indias, Indoneesias, Itaalias, Jaapanis, Kanadas, Keenias, Korea Vabariigis, Lõuna-Aafrika Vabariigis, Mehhikos, Nigeerias, Pakistanis, Poolas, Prantsusmaal, Rootsis, Saksamaal, Suurbritannias, Tuneesias, Türgis ja Venemaal.

55 Euroopa Nõukogu 28. jaanuari 1981. aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (ETS nr 108) ning isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni järelevalveasutusi ja andmete piiriülest liikumist käsitlev 2001. aasta lisaprotokoll (ETS nr 181). See on andmekaitse valdkonnas ainus siduv mitmepoolne dokument. Viimati on konventsiooni ratifitseerinud Argentina, Mehhiko, Cabo Verde ja Maroko.

56 Ministrite komitee 17.–18. mai 2018 Taanis Helsingøris toimunud 128. istungjärgul kokkulepitud protokoll, millega muudetakse konventsiooni üksikisikute kaitse kohta isikuandmete automatiseeritud töötlemisel (ETS nr 108). Konventsiooni ajakohastatud versiooni konsolideeritud tekst asub aadressil https://rm.coe.int/16808ade9d.

2017. aasta jaanuari teatises „Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas“[57] esitatud strateegia rakendamisega tihendas komisjon suhtlust kolmandate riikide ja teiste rahvusvaheliste partneritega, keskendudes privaatsussüsteemide veelgi suuremale ühtlustamisele. See hõlmas ka kaitse piisavuse otsuste kasutamise võimalust valitud kolmandate riikide puhul.[58] See töö on andnud olulisi tulemusi, nagu 2019. aasta veebruaris ELi ja Jaapani vahel jõustunud andmekaitse piisavuse vastastikuse tunnustamise kokkulepe, mille alusel loodi maailma suurim andmete vaba ja turvalise liikumise ala. Sarnased läbirääkimised Lõuna-Koreaga on lõpusirgel ning ettevalmistamisel on kokkulepped mitme Ladina-Ameerika riigiga (nt Tšiili ja Brasiiliaga), kelle puhul oleneb edasine koostöö pooleliolevast õigusloome protsessist. Lootustandev on olukord ka Aasia teatavates osades (Indias, Indoneesias ja Taiwanis) ning ELi ida- ja lõunanaabruses, kus võib samuti avaneda võimalusi kaitse piisavuse läbirääkimiste alustamiseks.

Ühtlasi on komisjonil hea meel selle üle, et teised riigid, kes on kasutusele võtnud määruses sätestatud kaitse piisavuse otsustega sarnased süsteemid, tunnistavad ELi ja sellelt asjaomase heakskiidu saanud riikide andmekaitse piisavust.[59] Selle põhjal on võimalik luua riikide võrgustik, kus andmed saavad vabalt liikuda.

Lisaks tehakse palju tööd selle nimel, et kaitse piisavuse otsus jääks kehtima nende kolmandate riikide puhul, kelle suhtes see langetati 1995. aasta andmekaitsedirektiivi alusel (Argentina, Iisrael, Kanada ja Uus-Meremaa). Samal ajal on kasulikuks abivahendiks ka ELi ja Ameerika Ühendriikide ühine andmekaitseraamistik Privacy Shield, mis kaitseb enam kui 4700 ettevõttega toimuvat atlandiülest andmevahetust.[60] See vaadatakse kord aastas läbi ja seetõttu saab uued probleemid kiiresti lahendada, et kõik toimiks korralikult.

Kuna andmeedastuse jaoks ei ole olemas kõigile ühtmoodi sobivat lahendust, püüab komisjon koos sidusrühmade ja andmekaitsenõukoguga kasutada rahvusvahelise andmeedastuse jaoks täiel määral ära kõiki määruses sätestatud abivahendeid – lepingu tüüptingimusi, sertifitseerimissüsteeme, toimimisjuhendeid ja avaliku sektori asutuste halduskokkuleppeid. Sellega seoses on komisjon huvitatud kogemuste ja parimate tavade vahetamisest teiste süsteemidega, kus on ehk juba välja kujunenud konkreetne oskusteave mõne sellise abivahendi kohta. Komisjon kaalub, kas kasutada määrusega talle nende abivahenditega seoses antud volitusi, eriti lepingu tüüptingimuste puhul.

Peale rangelt kahepoolsete vahendite võiks uurida, kas sarnaselt mõtlevad riigid ei saaks moodustada selles valdkonnas ühist õigusraamistikku, sest praegusel ajal on andmed kaubanduses, kommunikatsioonis ja sotsiaalses suhtluses üha olulisem komponent. Kui hinnatakse samu väärtusi ja süsteemid ühtlustatakse, saaks andmed osaliste vahel vabalt liikuda, olles ühtlasi piisavalt kaitstud. Ühise õigusraamistiku loomisel võiks toetuda näiteks

---

[57] Komisjoni teatis Euroopa Parlamendile ja nõukogule „Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas“ (COM(2017) 07 final).

[58] Määrusega on loodud võimalus teha kaitse piisavuse otsuseid ka rahvusvaheliste organisatsioonide suhtes, kellega EL soovib andmeid vahetada.

[59] Sellist süsteemi kasutavad näiteks Argentina, Colombia, Iisrael ja Šveits.

[60] See tähendab, et Privacy Shieldiga on selle kolme toimimisaasta jooksul ühinenud rohkem ettevõtteid kui selle eelkäijaga (Safe Harbour) 13 aastaga.

ajakohastatud konventsioonile nr 108 või otsida inspiratsiooni Jaapanis selle aasta alguses käivitatud andmete usaldusväärse vaba liikumise algatusest.

Uus sünergia kaubanduse ja andmekaitse vahel

Andmekaitsenormide rahvusvahelise ühtlustamise kõrval tahab komisjon võidelda ka digitaalse protektsionismi vastu. Selleks on kaubanduskokkulepete jaoks koostatud spetsiaalsed andmeedastuse ja -kaitse sätted, mida pakutakse alati välja nii kahe- kui ka mitmepoolsetel läbirääkimistel (nt praegustel WTO e-kaubanduse läbirääkimistel). Need n-ö horisontaalsed sätted välistavad protektsionismi (nt andmete sundlokaliseerimise nõuded), takistamata siiski osaliste õigusloomelist autonoomiat tagada andmekaitse põhiõigus.

Kuigi läbirääkimised andmekaitse ja kaubanduse üle peavad toimuma eraldi, võivad nad siiski teineteist täiendada: parim näide sellisest sünergiast on ELi ja Jaapani andmekaitse piisavuse vastastikuse tunnustamise kokkulepe, mis lihtsustab veelgi ärilist andmevahetust ja suurendab nii majanduspartnerluslepingust saadavat kasu. Selline ühistel väärtustel ja rangetel normidel põhinev ühtlustamine, mida toetavad tulemuslikud täitmismeetmed, loob tugevaima aluse isikuandmete vahetamiseks ning seda tunnistavad järjest enam ka meie välispartnerid.[61] Kuna ettevõtted tegutsevad üha enam piiriüleselt ja eelistavad järgida kõikjal maailmas ühetaolisi reegleid, loob andmekaitse ühtlustumine soodsa keskkonna otseinvesteeringute jaoks, lihtsustab kaubavahetust ja suurendab äripartnerite omavahelist usaldust.

Kuritegevuse ja terrorismi vastane teabevahetus on lihtsam, kui kasutada sobivaid kaitsemeetmeid

Eri riikide andmekaitsekorra suurem ühilduvus võib lihtsustada ka väga vajalikku teabevahetust ELi ja välismaiste ameti-, politsei- ja kohtuvõimude vahel ning nii aidata kaasa õiguskaitsealase koostöö tulemuslikumaks ja tõhusamaks muutumisele.[62] Selleks kavatseb komisjon kasutada õiguskaitsealase andmekaitse direktiiviga ette nähtud kaitse piisavuse otsuseid, et süvendada oma olulisimate partneritega kuritegevuse ja terrorismi vastast koostööd. Peale selle saab teiste oluliste julgeolekupartneritega sarnaste kokkulepete sõlmimisel eeskujuks võtta 2017. aasta veebruaris jõustunud ELi ja USA vahelise raamkokkuleppe[63].

---

61 Näiteks viidatakse Osakas toimunud G20 kohtumisel koostatud riigijuhtide deklaratsioonis andmete usaldusväärse vaba liikumise mõistele: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

62 Vt komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa julgeoleku tegevuskava“ (COM(2015) 185 final).

63 ELi ja USA vaheline isikuandmete kaitse kokkulepe, milles käsitletakse kriminaalasjades tehtava politsei- ja õigusalase koostöö raames süütegude, sealhulgas terrorismi tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise eesmärgil edastatavate ja töödeldavate isikuandmete kaitset: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A22016A1210%2801%29 (edaspidi „raamlepe“). Raamlepe on esimene kahepoolne rahvusvaheline õiguskaitsealane kokkulepe, mis sisaldab põhjalikku loetelu andmekaitsealastest õigustest ja kohustustest kooskõlas ELi õigusega. See on suurepärane näide sellest, kuidas rangetes andmekaitsemeetmetes kokkuleppimisega saab tõhustada õiguskaitsealast koostööd tähtsa rahvusvahelise partneriga.

Teised näited, mis toovad esile rangete andmekaitsenormide olulisuse kolmandate riikidega tehtavas õiguskaitsealases koostöös, on broneeringuinfo edastamine[64] ning operatiivinfovahetus Europoli ja oluliste rahvusvaheliste partnerite vahel. Sellega seoses on käimas või ettevalmistamisel läbirääkimised rahvusvaheliste kokkulepete sõlmimiseks mitme lõunanaabruses asuva riigiga.[65]

Tugevad andmekaitsemeetmed saavad olema ka kõigi selliste tulevaste lepingute lahutamatu osa, mis sõlmitakse kriminaaluurimises elektrooniliste tõendusmaterjalidega piiriülese tutvumise kohta nii kahe- (ELi ja USA leping) kui ka mitmepoolselt (Euroopa Nõukogu (Budapesti) küberkuritegevuse konventsiooni teine lisaprotokoll).[66]

Andmekaitsenõuete täitmise tagajate koostöö edendamine

Ajal, mil privaatsusnõuete täitmise probleemid või turvaintsidendid võivad mõjutada üheaegselt paljusid inimesi eri riikides, võib järelevalveasutuste tihedam rahvusvaheline koostöö aidata kaasa nii konkreetsete õiguste tõhusamale kaitsele kui ka stabiilsema ettevõtluskeskkonna loomisele. Seda arvestades otsib komisjon tihedas koostöös andmekaitsenõukoguga võimalusi, kuidas lihtsustada täitmise tagamise alast koostööd ja vastastikust abi ELi ja välismaiste järelevalveasutuste vahel, kasutades muu hulgas määrusega selleks antud uusi volitusi.[67] See võib hõlmata eri liiki koostööd alates ühiste tõlgendus- või praktiliste vahendite[68] väljatöötamisest kuni teabevahetuseni käimasolevate uurimiste kohta.

Samuti kavatseb komisjon kiirendada dialoogi piirkondlike organisatsioonide ja võrgustikega (Kagu-Aasia Maade Assotsiatsioon ASEAN, Aafrika Liit, Aasia Vaikse ookeani piirkonna privaatsusametite foorum APPA ja Ladina-Ameerika andmekaitsevõrgustik), kes on üha tähtsamad ühiste andmekaitsenormide kujundajad, parima tava levitamise edendajad ja täitmise tagajate vahelise koostöö soodustajad. Komisjon teeb koostööd ka Majanduskoostöö ja Arengu Organisatsiooniga OECD ning Aasia ja Vaikse ookeani piirkonna riikide majanduskoostöö organisatsiooniga, et saavutada kõikjal sarnane kõrge andmekaitsetase.

VII. Andmekaitsenormid kui paljude poliitikavaldkondade lahutamatu osa

Isikuandmete kaitse on lõimitud paljudesse liidu poliitikavaldkondadesse.

Telekommunikatsioon ja elektroonilise side teenused

---

64 ÜRO Julgeolekunõukogu 21. detsembri 2017. aasta resolutsioonis nr 2396 kutsutakse kõiki ÜRO liikmesriike üles arendama välja broneeringuinfo kogumise, töötlemise ja analüüsimise võimekust, arvestades täiel määral ka inimõiguste ja põhivabadustega. Vt ka komisjoni teatis „Euroopa julgeoleku tegevuskava“ (COM(2015) 185 final): https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52015DC0185&qid=1566509913461&from=ET.

65 https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en.

66 http://europa.eu/rapid/press-release_IP-19-2891_en.htm.

67 Vt määruse artikkel 50 rahvusvahelise andmekaitsealase koostöö kohta. See hõlmab paljusid erinevaid koostöövorme alates andmekaitsealaste õigusaktide kohta teabe jagamisest kuni kaebuste edastamise ja uurimisabini.

68 Nt ühised rikkumisteatiste vormid.

Komisjon esitas privaatsuse ja elektroonilise side määruse ettepaneku 2017. aasta jaanuaris.[69] Ettepaneku eesmärk on kaitsta side konfidentsiaalsust (nagu on nõutud põhiõiguste hartas), aga ka sidesüsteemides liikuda võivaid isikuandmeid ja lõppkasutajate lõppseadmeid.

Kavandatav internetiprivaatsuse määrus täpsustab ja täiendab isikuandmete kaitse üldmäärust, sätestades eelmainitu jaoks konkreetsed eeskirjad. Sellega ajakohastatakse ELi praegusi internetiprivaatsuse eeskirju[70], võttes arvesse tehnoloogia ja õigusnormide arengut. Sellega suurendatakse inimeste privaatsust, laiendades uute eeskirjade kohaldamisala ka internetipõhiste kommunikatsiooniteenuste (OTT-teenused) osutajatele, luues nii võrdsed võimalused kõigi elektroonilise side teenuste jaoks. Kuigi Euroopa Parlament võttis 2017. aasta oktoobris vastu kolmepoolsete läbirääkimiste algatamise volitused, ei ole nõukogu veel üldises lähenemisviisis kokkuleppele jõudnud. Komisjon jääb internetiprivaatsuse määrusele kindlaks ja toetab kaasseadusandjaid, et see kiiresti vastu võetud saaks.

Tervishoid ja uurimistegevus

Terviseandmete kui määruse mõistes tundlike andmete jagamise lihtsustamine liikmesriikide vahel muutub tervishoius avalike huvidega seotud põhjustel üha olulisemaks. Sellised avalikud huvid on tervishoiuteenuste osutamine, kaitse tõsiste piiriüleste terviseohtude eest ning tervishoiuteenuste, ravimite ja meditsiiniseadmete ranged ohutus- ja kvaliteedinormid. Määruses on sätestatud eeskirjad, mis tagavad terviseandmete töötlemise ja jagamise seaduslikkuse ja usaldusväärsuse ELis. Neid kohaldatakse ka olukordades, kus kolmandad isikud kasutavad (sh teadusuuringuteks) patsientide terviseandmeid (patsientide tervisekaardid, digiretseptid ja pikemas perspektiivis üleüldse kõik elektroonilised terviseandmed). Kliiniliste uuringute jaoks on komisjon koostanud kliiniliste uuringute määruse[71] ja isikuandmete kaitse üldmääruse koosmõju kohta küsimuste ja vastuste dokumendi[72].

Tehisintellekt

Kuna tehisintellekt muutub strateegiliselt üha tähtsamaks, tuleb selle arendamise ja kasutamise jaoks kujundada üleilmsed reeglid. Komisjon toetab tehisintellekti arendamist ja kasutuselevõttu edendades inimkesksuse põhimõtet, mille kohaselt peavad tehisintellekti rakendused olema kooskõlas põhiõigustega.[73] Määruses sätestatud eeskirjad loovad selleks

---

69 https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52017PC0010.

70 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 37–47.

71 https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A32014R0536.

72 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.

73 Komisjoni 8. aprilli 2019. aasta teatis „Usalduse loomine inimkeskse tehisintellekti vastu“: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52019DC0168&qid=1566786273960&from=EN. Kõrgetasemelise eksperdirühma 8. aprilli 2019. aasta eetikasuunised usaldusväärse tehisintellekti jaoks: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Vt ka OECD nõukogu soovitust tehisintellekti kohta: (https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449), G20 põhimõtted tehisintellekti jaoks Osakas toimunud kohtumisel koostatud riigi juhtide deklaratsioonis (https://www.g20.org/pdf/documents/en/annex_08.pdf) ning G20 ministrite avaldus kaubanduse ja

vajaliku üldraamistiku ning sisaldavad ka konkreetseid kohustusi ja õigusi, mida tuleb tehisintellekti abil isikuandmete töötlemisel järgida. Näiteks on määrusega ette nähtud õigus, et inimese üle ei tohi otsuseid teha vaid masin (v.a teatavad olukorrad).[74] Samuti sisaldab see masina tehtud otsuste jaoks konkreetseid läbipaistvusnõudeid: kohustus sellistest otsustest inimesele teada anda, esitada otsustamise kohta sisulist teavet ning selgitada talle selle olulisust ja arvatavaid tagajärgi.[75] Neid määruse üldpõhimõtteid on tehisintellektist tingitud probleemide lahendamiseks ja võimaluste kasutamiseks oluliseks pidanud ka kõrgetasemeline tehisintellekti eksperdirühm[76], Majanduskoostöö ja Arengu Organisatsioon (OECD)[77] ja G20[78]. Euroopa Andmekaitsenõukogu on määranud tehisintellekti üheks võimalikuks 2019.–2020. aasta tööprogrammi teemaks.[79]

Transport

Andmesideühendusega autode ja arukate linnade arendamisel toetutakse üha enam suuremahuliste isikuandmete töötlemisele ja jagamisele mitme osapoole vahel (autod, autotootjad, telemaatikateenuse osutajad ja teetaristu eest vastutavad avaliku sektori asutused). Sellises mitme osalisega keskkonnas on mõnevõrra keeruline määrata isikuandmete töötlejate rolle ja kohustusi ning seda, kuidas tagada, et kõik töötlejad töötleks andmeid seadusega kooskõlas. Selleks et eri liiki arukate transpordisüsteemide kasutuselevõtt õnnestuks ning inimeste ja kaupade suuremat liikuvust võimaldavad digitaalsed vahendid ja teenused[80] leviks, on määruse ja internetiprivaatsuse õigusaktide järgimine hädavajalik.

Energeetika

Digitaalsete lahenduste loomisel energeetikasektoris toetutakse üha enam isikuandmete töötlemisele. Paketis „Puhas energia kõikidele eurooplastele“[81] on uued sätted, mis võimaldavad energeetikasektori digitaliseerimist, ning eeskirjad andmete juurdepääsetavuse, andmehalduse ja koostalitlusvõime jaoks, mis võimaldaks kasutada tarbijate reaalaja-andmeid säästmiseks ning omatootmisele ja energiaturul osalemisele ärgitamiseks. Seetõttu on nende sätete edukaks rakendamiseks vaja järgida andmekaitse-eeskirju.

---

digitaalmajanduse kohta (https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf).

74 Määruse artikkel 22.

75 Määruse artikli 13 lõike 2 punkt f.

76 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.

77 OECD nõukogu soovitus tehisintellekti kohta: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

78 G20 ministrite avaldus kaubanduse ja digitaalmajanduse kohta: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

79 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_et.pdf.

80 Nt sellised, mis lihtsustavad kavandamist ja eri transpordivahendite kasutamist reisi jooksul.

81 Eriti elektrituru direktiivis: https://eur-lex.europa.eu/legal-content/ET/ALL/?uri=CELEX%3A32009L0072.

Konkurents

Konkurentsipoliitikas tuleb üha enam arvestada isikuandmete töötlemisega.[82] Kuna andmekaitseasutused on ainsad asutused, kes võivad hinnata andmekaitse-eeskirjade rikkumisi, teevad konkurentsi-, tarbijakaitse- ja andmekaitseasutused praegu ja ka tulevikus oma pädevuste kokkupuutepunktides vajaduse korral koostööd. Komisjon soodustab sellist koostööd ja jälgib selle suundumusi hoolega.

Valimised

Valimisalase paketi[83] raames 2018. aasta septembris välja antud suunistes isikuandmete kasutamise kohta valimiste kontekstis[84] juhtis komisjon tähelepanu valimiste osaliste jaoks eriti olulistele eeskirjadele ja valijate individuaalse mõjutamise probleemidele. Suuniste sisu kajastus ka Euroopa Andmekaitsenõukogu avalduses[85] ja paljude riiklike andmekaitseasutuste suunistes. Valimisalane pakett sisaldas ka üleskutset, et iga liikmesriik looks valimistega seotud veebitegevuse jaoks oma riikliku võrgustiku, kuhu kuuluvad riigiasutused, kelle pädevuses on valimisküsimused ning andmekaitse- ja muude eeskirjade täitmise järelevalve ja tagamine. Samuti nähti uusi meetmeid, millega kehtestada Euroopa tasandi erakondade ja sihtasutuste jaoks sanktsioonid andmekaitse-eeskirjade rikkumise eest. Komisjon soovitas liikmesriikidel teha sama ka riigi tasandil. Andmekaitsega seotud aspekte vaadeldakse ka 2019. aastal toimunud Euroopa Parlamendi valimiste hindamisaruandes, mis peaks avaldatama 2019. aasta oktoobris.

Õiguskaitse

Tõeline ja tulemuslik julgeolekuliit on võimalik ainult siis, kui järgitakse täiel määral ELi hartas ja teisestes õigusaktides sätestatud põhiõigusi ning järgitakse ka sobivaid andmekaitsemeetmeid, mis võimaldavad isikuandmete turvalist jagamist õiguskaitse otstarbel. Privaatsuse kui põhiõiguse ja andmekaitsega seotud piirangute kehtestamisel tuleb rangelt järgida vajaduse ja proportsionaalsuse nõuet.

---

82 Nt juhtumid M.8788 – Apple/Shazam ja M. M.8124 – Microsoft/LinkedIn.

83 http://europa.eu/rapid/press-release_IP-18-5681_et.htm.

84 https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52018DC0638&qid=1566512482559&from=EN.

85 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

VIII. Kokkuvõte

Praeguseks kättesaadava teabe ja sidusrühmadega peetud dialoogi alusel saab komisjon öelda, et esialgsel hinnangul on määruse esimene kohaldamisaasta olnud üldjoontes positiivne. Sellegipoolest (ja nagu ka teatisest näha) on vaja veel edusamme mitmes valdkonnas.

Õigusraamistiku rakendamine ja täiendamine

- Need kolm liikmesriiki, kes ei ole veel oma riigi andmekaitseõigust ajakohastanud, peavad seda tegema võimalikult kiiresti. Kõik liikmesriigid peaksid viima oma valdkondlikud õigusaktid määruse nõuetega täielikult kooskõlla.

- Komisjon kasutab kõiki oma käsutuses olevaid võimalusi (sh rikkumismenetlusi), et liikmesriigid järgiksid määrust ning et andmekaitse õigusraamistikus oleks killustatust võimalikult vähe.

Uue juhtimissüsteemi kogu potentsiaal tuleb kasutusele võtta

- Liikmesriigid peaksid hoolitsema selle eest, et nende andmekaitseasutustel oleks piisavalt töötajaid, raha ja tehnilisi vahendeid.

- Andmekaitseasutused peaksid tegema rohkem koostööd (nt korraldama ühisuurimisi). Liikmesriigid peaksid selliseid uurimisi soodustama.

- Andmekaitsenõukogu peaks ELi andmekaitsekultuuri edasi arendama ja kasutama kõiki määruses sätestatud vahendeid, mille abil tagada eeskirjade ühtne kohaldamine. Samuti peaks nõukogu jätkama suuniste koostamist, eriti VKEdele.

- Andmekaitsenõukogu sekretariaadi erialast ettevalmistust tuleks parandada, et see saaks nõukogu tööd rohkem toetada ja juhtida.

- Komisjon jätkab andmekaitseasutuste ja andmekaitsenõukogu abistamist, osaledes aktiivselt nõukogu töös ja juhtides määruse rakendamise käigus selle tähelepanu ELi õiguse nõuetele.

- Komisjon toetab andmekaitseasutuste suhtlust teiste asutustega (eriti konkurentsiasutustega), austades täiel määral nende valdkondlikku pädevust.

Sidusrühmade abistamine ja kaasamine

- Andmekaitsenõukogu peaks sidusrühmi oma töösse rohkem kaasama. Komisjon jätkab andmekaitseasutuste rahalist toetamist sidusrühmadega suhtlemisel.

- Komisjon jätkab teavitustegevust ja muud sidusrühmadega seotud tööd.

Rahvusvaheline lähendamine

- Komisjon intensiivistab kvalifitseeruvate partneritega peetavat dialoogi kaitse piisavuse valdkonnas (sh õiguskaitses). Täpsemalt soovitakse lähikuudel lõpule viia Lõuna-Koreaga peetavad läbirääkimised. 2020. aastal esitab komisjon aruande andmekaitsedirektiivi alusel tehtud 11 kaitse piisavuse otsuse läbivaatamise kohta.
- Komisjon jätkab tööd (sh tehnilise abi andmist ning teabe ja parimate tavade vahetamist) kolmandate riikidega, kes on huvitatud tänapäevaste privaatsuseeskirjade vastuvõtmisest, ning soodustab koostööd kolmandate riikide järelevalveasutuste ja piirkondlike organisatsioonidega.
- Komisjon suhtleb mitmepoolsete ja piirkondlike organisatsioonidega, et edendada andmekaitsenorme kui kaubanduse ja koostöö soodustajaid (nt G20 kohtumisel Jaapani käivitatud andmete usaldusväärse vaba liikumise algatuse raames).

Määruse kohaselt[86] peab komisjon selle rakendamisest 2020. aastal aru andma. Selle käigus saab hinnata tehtud edusamme ja seda, kas uue andmekaitsekorra eri komponendid pärast kaheaastast kohaldamist täielikult toimivad. Selleks suhtleb komisjon Euroopa Parlamendi, nõukogu, liikmesriikide, Euroopa Andmekaitsenõukogu, sidusrühmade ja kodanikega.

[86] Määruse artikkel 97.