



Brüssel, 10.1.2017
COM(2017) 7 final

KOMISJONI TEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE

Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas

1. SISSEJUHATUS

Isikuandmete kaitse kuulub Euroopa ühiste põhiseaduslike väärtuste hulka ja see on sätestatud ELi põhiõiguste harta artiklis 8. Isikuandmete kaitse on olnud ELi õiguses kesksel kohal üle 20 aasta, alates 1995. aasta andmekaitse direktiivist¹ (edaspidi „1995. aasta direktiiv”) kuni isikuandmete kaitse üldmääruse² ja politseidirektiivi³ vastuvõtmiseni 2016. aastal.

President Juncker rõhutas oma kõnes olukorrast Euroopa Liidus 14. septembril 2016: „[o]lla eurooplane tähendab õigust oma isikuandmete kaitsele tugevate Euroopa seaduste kaudu. [...] Privaatsus on Euroopas oluline. See on inimväärikuse küsimus.”

Kuid mitte ainult eurooplased ei soovi oma isikuandmeid kaitsta. Tarbijad kõikjal maailma hindavad ja väärtustavad privaatsust üha enam. Ettevõtjad omakorda tajuvad, et tugev privaatsuse kaitse annab neile konkurentsieelise, kuna see suurendab usaldust nende teenuste vastu. Paljud neist, eeskätt ülemaailmse haardega firmad, joonduvad privaatsuse kaitse põhimõtetes isikuandmete kaitse üldmäärusest nii sellepärast, et nad tahavad ELis tegutseda, kui ka sellepärast, et näevad üldmääruses järgimisväärset eeskuju.

Samuti võtavad mitu riiki ja piirkondlikku organisatsiooni väljaspool ELi, meie lähimatest naabritest kuni Aasia, Ladina-Ameerika ja Aafrikani vastu uusi isikuandmete kaitset käsitlevaid õigusakte või ajakohastavad kehtivaid õigusakte, selleks et ära kasutada globaalse digitaalmajanduse võimalusi ning tulla vastu kasvavale nõudlusele tugevama andmeturbe ja privaatsuse kaitse järele. Kuigi riigid lähenevad probleemidele erinevalt ja nende seadusandliku arengu tase on erinev, on siiski näha üldist ühtlustumist oluliste isikuandmete kaitse põhimõtetega, eelkõige teatavates maailma piirkondades⁴. Suurem koosõla erinevate andmekaitse süsteemide vahel hõlbustaks isikuandmete rahvusvahelist edastamist nii ettevõtlusega seotud eesmärkidel kui ka riikide ametiasutuste (nt õiguskaitseasutuste) vahelises koostöös. EL peaks haarama võimalusest edendada oma andmekaitsealaseid väärtusi ja soodustada andmevoogusid, toetades õigussüsteemide lähenemist. Nagu on öeldud komisjoni tööprogrammis,⁵ esitatakse käesolevas teatises komisjoni strateegiline raamistik kaitse piisavuse otsuste ning muude andmete edastamise vahendite ja rahvusvaheliste andmekaitsealaste õigusaktide kasutamiseks.

¹ Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, 23.11.95).

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 1–88). Määrus jõustus 24. mail 2016 ja seda hakatakse kohaldama alates 25. maist 2018.

³ 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, lk 89–131). Direktiiv jõustus 5. mail 2016. Liikmesriigid peavad selle oma õigusesse üle võtma 6. maiks 2018.

⁴ Vt „Data protection regulations and international data flows: Implications for trade and development”, ÜRO Kaubandus- ja Arengukonverents UNCTAD (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

⁵ Komisjoni 2017. aasta tööprogramm. Luues Euroopat, mis hoiab, kaitseb ja avardab võimalusi, COM(2016) 710 (final), 25.10.2016, lk 12 ja 1. lisa.

2. ELI ANDMEKAITSE REFORMIPAKETT — TÄNAPÄEVANE SEADUSANDLIK RAAMISTIK, MIS TOETAB RAHVUSVAHELISI HÄSTI KAITSTUD ANDMEVOOGUSID

2016. aasta aprillis vastuvõetud ELi andmekaitsealaste õigusaktide reformiga loodi süsteem, mis ühest küljest tagab andmetele tugeva kaitse ja teisest küljest on avatud globaalse infoühiskonna võimalustele. Andes inimestele oma isikuandmete üle suurema kontrolli, suurendab reform tarbijate usaldust digitaalmajanduse vastu. Õiguskeskkonda ühtlustades ja lihtsustades muudab reform ettevõtlusega tegelemise ELis nii ELis asutatud kui ka ELi-väliste äriühingute jaoks hõlpsamaks ja vähem koormavaks, muuhulgas andmete rahvusvahelise vahetamise kaudu. Praegu on EL avatud rahvusvahelistele andmevoogudele, tagades üksikisikutele samal ajal kõrgeima kaitse taseme. ELil on potentsiaali saada andmeteenuste keskuseks, mille eeldusteks on vabad andmevood ja usaldus.

2.1 Kõikehõlmav, ühtne ja lihtsustatud ELi andmekaitse raamistik

ELi reformiga kehtestatakse kõikehõlmav raamistik, mis reguleerib isikuandmete töötlemist nii avalikus kui ka erasektoris ning nii ettevõtluse kui ka õiguskaitse valdkonnas (vastavalt isikuandmete kaitse üldmäärus ja politseidirektiiv).

Isikuandmete kaitse üldmääruse kohaselt hakkab alates 2018. aasta maist kehtima üks üleeuroopaline õigusnormide kogum, mitte 28 eri riigi seadused nagu praegu. Uus ühtse kontaktpunkti mehhanism tagab, et kui ettevõtte teeb ELis piiriüleseid andmetöötlustoiminguid, vastutab järelevalve eest üks andmekaitseasutus. Tagatud on uute õigusnormide järjepidev tõlgendamine. Eeskätt selliste piiriüleste juhtumite puhul, millega tegelevad mitu liikmesriigi andmekaitseasutust, tehakse üks otsus, tagamaks, et ühistele probleemidele leitakse ühised lahendused. Lisaks sellele loob isikuandmete kaitse üldmäärus võrdsed võimalused ELi ja ELi-välistele ettevõtetele selles mõttes, et väljaspool ELi asuvad äriühingud peavad järgima samu norme kui Euroopa äriühingud, kui nad pakuvad kaupu ja teenuseid või jälgivad üksikisikute käitumist ELis. Tarbijate suurem usaldus toob kasu nii ELi kui ka ELi-välistele ettevõtjatele.

Politseidirektiivis on sätestatud ühised õigusnormid, mis reguleerivad üksikisikute andmete töötlemist kriminaalmenetluses, olgu see üksikisik kahtlustatav, kannatanu või tunnistaja, võttes arvesse politseitöö ja kriminaalasjades õigusmõistmise eripära. Andmekaitsenormide, sealhulgas andmete rahvusvahelist edastamist reguleerivate normide ühtlustamine õiguskaitse valdkonnas hõlbustab piiriülest koostööd politsei- ja õigusasutuste vahel nii ELi siseselt kui ka rahvusvaheliste partneritega ning aitab seega luua tingimused kuritegevusevastase võitluse tõhustamiseks. See on Euroopa julgeoleku tegevuskava⁶ oluline osa.

2.2 Uuendatud ja mitmekesine tööriistakast andmete rahvusvaheliseks edastamiseks

ELi andmekaitsealased õigusaktid on algusest peale sisaldanud mitut mehhanismi, mis võimaldavad andmeid rahvusvaheliselt edastada. Nende normide põhieesmärk on tagada, et kui eurooplaste isikuandmeid edastatakse väljapoole Euroopa Liitu, läheb isikuandmete kaitse

⁶ Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa julgeoleku tegevuskava”, COM(2015) 185 (final), 28.4.2015.

andmetega kaasa. Aastate jooksul on need normid võetud eeskujuks rahvusvaheliste andmevoogude reguleerimisel mitmes õigusruumis. Ehkki normide struktuur jääb põhiolemuselt samasuguseks nagu 1995. aasta direktiivis, selgitatakse ja lihtsustatakse reformiga andmete rahvusvahelise edastamise normide kasutust ning võetakse kasutusele uusi vahendeid andmete edastamiseks.

ELi õiguse kohaselt on üks võimalus isikuandmete edastamiseks väljapoole ELi tugineda komisjoni kaitse piisavuse otsusele, millega on kinnitatud, et isikuandmete kaitse tase kolmandas riigis on „sisuliselt samaväärne”⁷ sellega, mis on tagatud ELis. Kui selline otsus on tehtud, tähendab see, et isikuandmeid võib vabalt sellesse kolmandasse riiki edastada, ilma et andmeeksportija peaks pakkuma täiendavaid tagatise või taotlema mingit luba. Täpselt ja üksikasjalikult on ette nähtud hulk elemente, mida komisjon peab ELi-välises õiguskorras sätestatud andmekaitsetaset hinnates arvesse võtma. Elementide loetelu on kättesaadav huvitatud riikidele ja rahvusvahelistele organisatsioonidele⁸. Komisjon saab nüüd teha kaitse piisavuse otsuseid ka õiguskaitse valdkonnas⁹. Lisaks sellele, arendades edasi 1995. aasta direktiivi kohaldamisel tekkinud praktikad, on reformiga sõnaselgelt lubatud teha selliseid otsuseid isikuandmete kaitse piisavuse kohta, mis käsitlevad osa kolmanda riigi territooriumist või konkreetset sektorit või tööstusharu kolmandas riigis (nn osaline piisavus)¹⁰.

Kaitse piisavuse otsuse puudumise korral saab isikuandmeid rahvusvaheliselt edastada hulga alternatiivsete vahendite alusel, millega nähakse ette asjakohased isikuandmete kaitse tagatised¹¹. Reformiga muudetakse ametlikuks võimalused kasutada olemasolevaid vahendeid nagu lepingu tüüptingimused¹² ja siduvad kontsernisisesed eeskirjad¹³ ning laiendatakse neid võimalusi. Näiteks võib tüüptingimusi lisada nüüd ELis asuva töötleva ja ELi-välise riigi töötleva vahelisse lepingusse (nn töötlevatevahelised standardsätted)¹⁴. Siduvaid

⁷ ELi kohtu otsus, 6.10.2015, kohtuasjas C-362/14 *Maximillian Schrems v Data Protection Commissioner*, punktid 73, 74 ja 96. Vt ka isikuandmete kaitse üldmääruse põhjendus 104 ja politseidirektiivi põhjendus 67, milles on viidatud sisulise vastavuse standardile.

⁸ Vt isikuandmete kaitse üldmääruse artikkel 45. Artikli 45 lõikes 2 on sätestatud, et komisjon peab arvesse võtma muu hulgas õigusriigi põhimõtet, inimõiguste ja põhivabaduste austamist ning asjaomaseid õigusakte, sealhulgas õigusakte, mis käsitlevad isikuandmete kaitset, avalikku julgeolekut, kaitset, riiklikku julgeolekut, karistusõigust ja riigiasutuste juurdepääsu isikuandmetele. Neid peavad täiendama tõhusad ja kohtulikult kaitstavad õigused, sealhulgas üksikisikute haldus- ja õiguskaitse, ning sõltumatu järelevalveasutus, mis tagab andmekaitsestandardite järgimise ja täitmise. Arvesse võetakse ka õiguslikult siduvate konventsioonide, eelkõige Euroopa Nõukogu konventsiooni 108 nõuete täitmist ja isikuandmete kaitsega tegelevates mitmepoolsetes või piirkondlikes süsteemides osalemist.

⁹ Vt politseidirektiivi artikli 36 lõige 2 – kaitse piisavuse hindamisel arvesse võetavad konkreetsed asjaolud.

¹⁰ Vt isikuandmete kaitse üldmääruse artikli 45 lõige 1 ja politseidirektiivi artikli 36 lõige 1.

¹¹ Vt nt komisjoni teatis Euroopa Parlamendile ja nõukogule isikuandmete edastamise kohta ELis Ameerika Ühendriikidesse direktiivi 95/46/EÜ alusel pärast Euroopa Kohtu otsust kohtuasjas C-362/14 (*Schrems*), COM(2015) 566 (final), 6.11.2015.

¹² Lepingu tüüptingimustes sätestatakse vastavalt ELi eksportija ja kolmanda riigi importija andmekaitsealased kohustused.

¹³ Siduv kontsernisisene eeskiri on rahvusvahelise äriühingute kontserni poolt vastuvõetud sise-eeskiri, mis reguleerib andmete edastamist kontserni kuuluvatele üksustele, mis asuvad riikides, kus isikuandmete piisav kaitse tase ei ole tagatud. Kui siduvaid kontsernisisesid eeskirju võis kasutada juba 1995. aasta direktiivi kohaselt, siis isikuandmete kaitse üldmäärusega kodifitseeritakse nende kasutamine andmete edastamise vahendina ja muudetakse see ametlikuks.

¹⁴ Vt isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktid c ja d ning põhjendus 168.

kontsernisisesid eeskirju on siiani saanud kasutada ainult ühte kontserni kuuluvad üksused, kuid nüüd võib neid kasutada ka ettevõtjate rühm, kes tegeleb ühise majandustegevusega, kuid ei kuulu tingimata samasse kontserni¹⁵. Reformiga vähendatakse ka bürokraatiat, kuna sellega tühistatakse üldised nõuded teavitada andmekaitseasutusi eelnevalt isikuandmete edastamisest kolmandasse riiki lepingu tüüptingimuste või siduvate kontsernisest alusel ja taotleda andmekaitseasutuselt selleks luba¹⁶. See lihtsustab ELi andmete rahvusvahelise edastamise süsteemi oluliselt, kuna selliseid nõudeid, mis praegu on liikmesriikides erinevad, nähakse sageli suure takistusena andmevoogude teel, eriti väiksemate ettevõtete jaoks¹⁷.

Lisaks võetakse reformiga kasutusele uued vahendid andmete rahvusvaheliseks edastamiseks¹⁸. Vastutavad töötajad ja volitatud töötajad saavad teatavatel tingimustel¹⁹ kasutada heakskiidetud toimimisjuhendeid ja sertifitseerimismehhanisme, nagu näiteks privaatsusmargised, selleks et tõendada asjakohaste kaitsemeetmete olemasolu. See peaks võimaldama andmete rahvusvahelise edastamise jaoks individuaalsemate lahenduste väljatöötamist, mis vastaksid näiteks konkreetse sektori või tööstusharu või konkreetsete andmevoogudega seotud erinõuetele. Samuti on nüüd võimalik sätestada asjakohased kaitsemeetmed andmete edastamise puhul avaliku sektori asutuste või organite vahel rahvusvaheliste lepingute või halduskokkulepete põhjal²⁰. Ühtlasi on isikuandmete kaitse üldmääruses selgitatud nn erandite²¹ kasutamist (nt nõusolek, lepingu täitmine ja avalikust huvist tulenevad kaalukad põhjused), millele üksused saavad konkreetsetes olukordades andmete edastamisel tugineda kaitse piisavuse otsuse puudumise korral ja olenemata eelnimetatud vahendite kasutamisest. Üldmäärus sisaldab ka uut, kuigi piiratud erandit, mis puudutab andmete edastamist äriühingu õigustatud huvide²² elluviimiseks.

Reformiga on komisjonile antud volitused töötada välja rahvusvahelised koostöömehhanismid, millega hõlbustada isikuandmete kaitset käsitlevate õigusaktide tõhusa täitmise tagamist, sealhulgas vastastikuse abi osutamise teel²³. Sellega tunnustatakse järelevalveasutuste vahelisest tihedamast rahvusvahelisest koostööst saadavat kasu, mis aitaks tagada üksikisiku õiguste tõhusama kaitse ja suurema õiguskindluse ettevõtjate jaoks.

¹⁵ Vt isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt b, artikkel 47 ja põhjendus 110.

¹⁶ Vt isikuandmete kaitse üldmääruse artikli 46 lõige 2.

¹⁷ Asjaolu, et registreerimiskohustused kujutavad endast kaubandustõkkeid paljude ettevõtjate, eelkõige VKEde jaoks, on välja toodud nt UNCTADi aruandes, lk 34.

¹⁸ Vt isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktid e ja f.

¹⁹ ELi-väline vastutav töötaja saab järgida ELi toimimisjuhendit või sertifitseerimismehhanismi, võttes endale lepinguga või muul õiguslikult siduval viisil siduvad ja täitmisele pööratavad kohustused kohaldada toimimisjuhendis või mehhanismis ettenähtud isikuandmete kaitse meetmeid. Vt isikuandmete kaitse üldmääruse artikli 42 lõige 2.

²⁰ Vt isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt a ja lõike 3 punkt b.

²¹ Vt isikuandmete kaitse üldmääruse artikkel 49.

²² Vt isikuandmete kaitse üldmääruse artikli 49 lõike 1 teine lõik.

²³ Vt isikuandmete kaitse üldmääruse artikkel 50.

3. ISIKUANDMETE RAHVUSVAHELINE EDASTAMINE ÄRISEKTORIS – KAUBANDUSE EDENDAMINE PRIVAATSUSE KAITSE ABIL

Privaatsuse tagamine on stabiilsete, turvaliste ja konkurentsivõimeliste globaalsete kaubavoogude eeltingimus. Privaatsusega ei saa kaubelda²⁴. Internet ning kaupade ja teenuste digiteerimine on maailmamajandust muutnud ning Euroopa äriühingud, nii suured kui ka väikesed, saavad kõigis sektorites iga päev andmeid, sealhulgas isikuandmeid üle piiride. Kuna äritegevuses tuleb üha enam tugineda isikuandmete voogudele, on privaatsus ja isikuandmete turvalisus muutunud tarbijate usalduse kujunemisel määrava tähtsusega teguriks. Näiteks tunnistavad kaks kolmandikku eurooplastest, et on mures sellepärast, et neil ei ole kontrolli andmete üle, mida nad internetis esitavad, ja pooled vastanutest kardavad pettuse ohvriks langeda²⁵. Samal ajal leiavad Euroopa ettevõtted mõningates kolmandates riikides tegutsedes, et neid takistavad järjest enam protektsionistlikud piirangud, mida ei saa õigustada privaatsusega seotud põhjendatud kaalutlustega.

On selge, et digiajastul ei saa soodustada rahvusvahelist kaubandust ilma edendamata samal ajal isikuandmete ranget kaitset. Kuigi isikuandmete kaitse üle kaubanduslepingutes läbi ei räägita,²⁶ pakub ELi andmete rahvusvahelise edastamise režiim, mida on eespool kirjeldatud, laialdaselt erinevaid võimalusi andmevoogude tagamiseks erinevates olukordades nii, et andmed on kindlalt kaitstud.

3.1 Kaitse piisavuse otsused

Kui kolmanda riigi suhtes on tehtud kaitse piisavuse otsus, tähendab see, et isikuandmeid võib EList vabalt sellesse kolmandasse riiki edastada, ilma et ELi andmeeksportija peaks rakendama täiendavaid kaitsemeetmeid või täitma lisatingimusi. Otsusega, et riigi õigussüsteem tagab isikuandmetele piisava kaitse taseme, kinnitatakse, et selle riigi süsteem on lähedane ELi liikmesriikidele. Selle tulemusena loetakse andmete edastamine sellesse riiki võrdväärseks ELi-sisese andmeedastusega, mis toob kaasa eelisjuurdepääsu ELi ühtsele turule ja avab ärikanaleid ELi ettevõtjatele. Nagu on eespool selgitatud, on sellise otsuse tegemise eelduseks asjaolu, et isikuandmete kaitse tase riigis on võrreldav (või „sisuliselt samaväärne”)²⁷ liidus tagatud kaitse tasemega. Otsuse tegemiseks hinnatakse põhjalikult kolmanda riigi süsteemi, sealhulgas õigusnorme, mis reguleerivad avaliku sektori asutuste juurdepääsu isikuandmetele õiguskaitse, riikliku julgeoleku ja muudel avaliku huvi eesmärkidel.

Samal ajal ei tähenda kaitse piisavuse nõue, et ELi õigusnorme tuleb punkt punktilt kopeerida, nagu kinnitas ka Euroopa Kohus 2015. aastal Schremsi kohtuasjas tehtud otsuses²⁸. Küsimus on pigem selles, kas asjaomane ELi-väline süsteem tervikuna tagab privaatsusõiguste sisu,

²⁴ Vt nt komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Kaubandus kõigile: vastutustundlikuma kaubandus- ja investeerimispoliitika poole”, COM(2015) 497 (final), 14.10.2015, lk 7.

²⁵ Eurobaromeetri eriuuring nr 431 – Andmekaitse, juuni 2015.

²⁶ President Junckeri poliitilised suunised: *Euroopa uus algus: minu tegevuskava töökohtade loomiseks ning majanduskasvu, õigluse ja demokraatlike muutuste tagamiseks*

²⁷ Vt allmärkus 7.

²⁸ Vrd Schremsi kohtuasjas tehtud otsus, punkt 74.

nende tõhusa rakendamise, teostatavuse ja järelevalve kaudu nõutava isikuandmete kaitse kõrge taseme. Siiani vastu võetud kaitse piisavuse otsused on näidanud, et komisjon võib lugeda piisavaks suurt hulka erinevaid privaatsuse tagamise süsteeme, mis esindavad erinevaid õigustraditsioone. Otsuseid on tehtud riikide kohta, kes on Euroopa Liidu ja selle liikmesriikidega tihedalt seotud (Šveits, Andorra, Fääri saared, Guernsey, Jersey, Mani saar), riikide kohta, kes on olulised kaubanduspartnerid (Argentina, Kanada, Iisrael, Ameerika Ühendriigid), ning riikide kohta, kes on andmekaitse normide arendamisel oma piirkonnas esirinnas (Uus-Meremaa, Uruguay).

Kanada ja Ameerika Ühendriikide kohta tehtud otsused on osalise piisavuse otsused. Kanada otsust kohaldatakse ainult Kanada isikuandmete kaitse ja elektrooniliste dokumentide seaduse kohaldamisalasse kuuluvate erasektori üksuste suhtes. Hiljuti vastuvõetud otsus, mis käsitleb ELi-USA andmekaitseraamistikku Privacy Shield,²⁹ on erijuhtum, kuna üldiste andmekaitsealaste õigusaktide puudumise tõttu USA-s³⁰ tugineb see osalevate äriühingute poolt võetud kohustustele kohaldada selle kokkuleppe rangeid andmekaitse nõudeid ja nende kohustuste täitmist on võimalik USA õiguse kohaselt nõuda. Lisaks sellele tugineb Privacy Shield USA valitsuse konkreetsetele kinnitustele ja tagatistele seoses andmetele juurdepääsu saamisega riikliku julgeoleku eesmärgil,³¹ tänu millele oli võimalik teha kaitse piisavuse otsus. Kõnealuste kohustuste täitmist jälgib komisjon tähelepanelikult, ka raamistiku toimimise iga-aastase läbivaatamise raames.

Viimastel aastatel on järjest rohkem riike maailmas vastu võtnud uusi õigusakte isikuandmete kaitse ja privaatsuse valdkonnas või on seda tegemas. 2015. aastaks olid andmekaitse seadused kehtestanud 109 riiki, mis on suur edasimineku, võrreldes 76 riigiga, kes olid seda teinud 2011. aasta keskpaigaks³². Lisaks sellele on umbes 35 riiki praegu andmekaitse seaduseid koostamas³³. Need uued või ajakohastatud seadused põhinevad enamasti teatavatel ühistel põhimõtetel, mille hulka kuuluvad muu hulgas isikuandmete kaitse õiguse tunnustamine põhiõigusena, üldise õigusakti vastuvõtmine selles valdkonnas, üksikisikule selliste privaatsusõiguste tagamine, mida on võimalik teostada ja kohtus kaitsta, ning sõltumatu järelevalveasutuse asutamine. Seega tekib uusi võimalusi, eelkõige kaitse piisavuse otsuste kaudu andmete edastamist veelgi soodustada, tagades jätkuvalt isikuandmete kaitse kõrgel tasemel.

Selleks, et kolmanda riigi isikuandmete kaitse tase tunnistatakse piisavaks, peavad ELi õiguse kohaselt kehtima selles riigis isikuandmete kaitset reguleerivad õigusnormid, mis on

²⁹ Rakendusotsus EL(2016) 1250, 12. juuli 2016.

³⁰ Komisjon kutsus USA-d liikuma põhjaliku privaatsuse ja andmekaitse süsteemi poole, mis võimaldaks pikemas perspektiivis kahe süsteemi ühtlustumist. Komisjoni teatis Euroopa Parlamendile ja nõukogule „Atlandi-ülesed andmevood: usalduse taastamine tugevate kaitsemeetmete kaudu”, COM(2016) 117 (final), 29.2.2016.

³¹ See tähendab eelkõige presidendi poliitikasuunist 28 (*Presidential Policy Directive*, PPD-28), millega on kehtestatud hulk piiranguid ja kaitsemeetmeid signaalilüure operatsioonidele, ja eraldi ombudsmani määramist ELi isikute selleteemaliste kaebuste lahendamiseks.

³² G. Greenleaf, „Global data privacy laws 2015: 109 countries, with European laws now in a minority”, (2015) 133 *Privacy Laws & Business International Report*, 14–17.

³³ UNCTADI uuring, lk 8 ja 42 (allmärkus 4 eespool).

võrreldavad ELi normidega³⁴. See puudutab nii isikuandmete suhtes kohaldatavat sisulist kaitset kui ka kolmandas riigis tehtavat asjakohast järelevalvet ja võimalusi oma õigusi kaitsta.

Andmekaitse piisavuse raamistiku kohaselt on komisjon seisukohal, et kui hinnatakse, milliste kolmandate riikidega tuleks arendada dialoogi kaitse piisavuse teemal, tuleks arvesse võtta järgmisi kriteeriume³⁵:

- i) ELi (tegelike või potentsiaalsete) kaubandussuhete ulatus antud kolmanda riigiga, sealhulgas vabakaubanduslepingu olemasolu või käimasolevad läbirääkimised;
- ii) EList pärinevate andmevoogude maht, mis kajastab geograafilisi ja/või kultuurilisi sidemeid;
- iii) kolmanda riigi eesrindlik roll privaatsuse ja andmekaitse vallas, mis võiks teistele sama piirkonna riikidele eeskujuks olla,³⁶ ning
- iv) üldised poliitilised suhted kõnealuse kolmanda riigiga, eelkõige seoses ühiste väärtushinnangute edendamise ja ühiste eesmärkide poole püüdlemisega rahvusvahelisel tasandil.

Neid kaalutlusi arvesse võttes hakkab komisjon aktiivselt suhtlema peamiste kaubanduspartneritega Ida- ja Kagu-Aasias, alustades Jaapanist ja Koreast 2017. aastal³⁷ ning jätkates Indiaga, olenevalt sellest, millised on India edusammud andmekaitse seaduste nüüdisajastamisel, aga ka Ladina-Ameerika, eelkõige Mercosuri riikide ja Euroopa naaberriikidega, kes on üles näidanud huvi isikuandmete kaitse piisavuse otsuse saamise vastu. Lisaks sellele suhtleb komisjon andmekaitse teemal hea meelega ka muude kolmandate riikidega, kes selle vastu huvi tunnevad. Arutelu võimaliku andmekaitse taseme piisavuse otsuse üle hõlmab ühest küljest ELi andmekaitse normide selgitamist (kui selleks on vajadus) ja teisest küljest uurimist, kuidas saaks kolmanda riigi seaduseid ja tavaid nende lähendada.

Mõningatel juhtudel võib kogu riiki hõlmava lähenemise asemel olla sobivam kasutada võimalust teha osaline kaitse piisavuse otsus või otsus kaitse piisavuse kohta ühes sektoris (nt finantsteenused või IT-sektor), milles võib käsitleda geograafilisi piirkondi või tööstusharusid, mis on kolmanda riigi majanduses olulisel kohal. Sellisel juhul tuleb arvesse võtta näiteks selliseid asjaolusid nagu privaatsusrežiimi sisu ja arendamise staadium (on see eraldi seadus, mitu seadust või eri sektoreid käsitlevad seadused jne), kolmanda riigi konstitutsiooniline ülesehitus ja kas EList pärit andmevood mõjutavad eriti teatavaid majandussektoreid.

³⁴ Sellela seoses võtab komisjon kaitse piisavuse hindamisel arvesse ka kolmanda riigi kohustusi, mis tulenevad õiguslikult siduvatest konventsioonidest, eelkõige seda, kas riik on ühinenud konventsiooniga 108 ja selle lisaprotokolliga. Vt isikuandmete kaitse üldmääruse artikli 45 lõike 2 punkt c ja põhjendus 105.

³⁵ Kui ELil on huvi teha riigiga koostööd sisejulgeoleku ja õiguskaitse vallas, uurib komisjon võimalusi teha kaitse piisavuse otsus politseidirektiivi kohaselt konkreetse olukorra kohta, vt punkt 4.

³⁶ See võib olla eriti asjakohane arengu- ja üleminekuriikidele, kuna isikuandmete kaitse on nii õigusriigi põhimõtte oluline osa kui ka majanduse konkurentsivõimet mõjutav tähtis tegur.

³⁷ Jaapan ja Korea on hiljuti vastu võtnud õigusaktid või neid nüüdisajastanud, et kehtestada põhjalikud isikuandmete kaitse süsteemid.

Kaitse piisavuse otsuse vastuvõtmiseks tuleb kolmanda riigiga avada eridialoog ja sisse seada tihe koostöö. Kaitse piisavuse otsused on „elavad” instrumendid, mille järgimist peab komisjon tähelepanelikult jälgima ja mida tuleb kohandada, kui toimuvad muutused, mis mõjutavad kolmanda riigi poolt tagatud isikuandmete kaitse taset³⁸. Selleks vaadatakse otsus korrapäraselt, vähemalt iga nelja aasta tagant läbi, et lahendada esilekerkivaid küsimusi ja vahetada lähedaste koostööpartneritega parimaid tavasid³⁹. Sellist dünaamilist lähenemisviisi kohaldatakse ka kehtivate, 1995. aasta direktiivi kohaselt vastu võetud kaitse piisavuse otsuste suhtes, mis tuleb läbi vaadata juhuks, kui need enam ei vasta kohaldatavatele nõuetele⁴⁰. Asjaomaseid kolmandaid riike kutsutakse seetõttu üles teavitama komisjoni mistahes asjakohasest muudatusest õigusnormides ja praktikas, mis on aset leidnud pärast nende kohta käiva kaitse piisavuse otsuse vastuvõtmist. See on vajalik selleks, et kaitse piisavuse otsused jääksid kehtima ka reformiga kehtestatud uute normide kohaselt⁴¹.

ELi andmekaitse normid ei saa olla vabakaubanduslepingu läbirääkimiste teema⁴². Kuigi andmekaitseteemaline dialoog ja kaubandusläbirääkimised kolmandate riikidega peavad toimuma eraldi, on kaitse piisavuse otsus, ka osaline või sektoripõhine kaitse piisavuse otsus parim viis vastastikuse usalduse loomiseks, kuna sellega tagatakse tõketeta andmevood, mis omakorda hõlbustavad äritehinguid, mis hõlmavad isikuandmete edastamist asjaomasesse kolmandasse riiki. Kaitse piisavuse otsused võivad seega kaubandusläbirääkimisi lihtsustada või juba sõlmitud kaubanduslepinguid täiendada nendest saadavat kasu võimendades. Kuna kaitse piisavuse otsus soosib kolmanda riigi andmekaitse taseme lähenemist ELis pakutavale tasemele, vähendab see samal ajal riski, et see riik hakkab isikuandmete kaitsele tuginedes kehtestama põhjendamatuid nõudeid andmete asukoha ja talletamise suhtes. Nagu on märgitud teatises „Kaubandus kõigile“, püüab komisjon lisaks sellele kasutada ELi kaubanduslepinguid, et kehtestada õigusnorme e-kaubanduse ja andmete piiriülese liikumise kohta ning tulla toime digitaalse proteksionismi uute ilmingutega, järgides täielikult ELi andmekaitse norme ja neid norme piiramata⁴³.

³⁸ Isikuandmete kaitse üldmääruse artikli 45 lõigetega 4 ja 5 on ette nähtud, et komisjon jälgib pidevalt suundumusi kolmandates riikides ja tal on õigus kaitse piisavuse otsus kehtetuks tunnistada, seda muuta või selle kehtivus peatada, kui ta leiab, et vastav riik ei taga enam isikuandmete kaitse piisavat taset.

³⁹ Isikuandmete kaitse üldmääruse artikli 45 lõige 3.

⁴⁰ Isikuandmete kaitse üldmääruse artikli 97 lõike 2 punkti a kohaselt peab komisjon 2020. aastaks esitama hindamisaruande Euroopa Parlamendile ja nõukogule.

⁴¹ Selleks, et teha järeldusi Schremsi kohtuasjas tehtud lahendist, milles leiti, et komisjon ületas oma volitusi, kui piiras andmekaitseasutuste õigust peatada või keelata andmete edastamine Safe Harbouri otsuse puhul, võttis komisjon 2016. aasta 16. detsembril vastu koondotsuse, millega kustutati sarnased sätted kehtivatest kaitse piisavuse otsustest ja asendati need sätetega, millega nähti ette üksnes nõue, et kui andmekaitseasutus keelab ajutiselt või alaliselt andmete edastamise kolmandasse riiki, siis peab liikmesriik komisjoni sellest teavitama. Koondotsusega on ette nähtud ka komisjoni kohustus jälgida kolmanda riigi õiguskorra arengut. Vt ELT L 344, 17.12.2016, lk 83.

⁴² Kaitse piisavuse otsus on eelkõige komisjoni ühepoolne rakendusotsus, mis on vastu võetud vastavalt ELi andmekaitse normidele, tuginedes nendes sätestatud kriteeriumitele.

⁴³ Vt komisjoni teatis „Kaubandus kõigile”, lk 12 (allmärkus 24 eespool).

Komisjon:

- alustab esmajärjekorras arutelusid võimalike kaitse piisavuse otsuste üle peamiste kaubanduspartneritega Ida- ja Kagu-Aasias, alustades Jaapanist ja Koreast 2017. aastal, kuid pidades silmas ka selliseid strateegilisi partnereid nagu India, ning Ladina-Ameerika, eelkõige Mercosuri riikide ja Euroopa naaberriikidega;
- jälgib tähelepanelikult kehtivate kaitse piisavuse otsuste toimimist. See hõlmab eelkõige ELi-USA andmekaitseraamistiku Privacy Shield rakendamist, eeskätt iga-aastase ühise läbivaatusmehhanismi kaudu;
- teeb koostööd riikidega, kes on huvitatud tugevate andmekaitse seaduste vastuvõtmisest, ja abistab neid ning toetab nende andmekaitse normide lähenemist ELi andmekaitse põhimõtetele.

3.2 Isikuandmete edastamise alternatiivsed mehhanismid

Isikuandmete kaitset reguleerivate ELi õigusnormide puhul on alati mööndud, et isikuandmete rahvusvahelisele edastamisele ei saa kohaldada tüüplahendusi. See vastab veelgi enam tõele reformiga kehtestatud õigusnormide puhul. Kuigi kaitse piisavuse otsuse saab teha ainult selliste kolmandate riikide kohta, kes vastavad asjaomastele kriteeriumitele, siis isikuandmete kaitse üldmäärus sisaldab mitu erinevat mehhanismi, mis on piisavalt paindlikud, et neid kohandada erinevatele olukordadele, kus on vaja isikuandmeid edastada. On võimalik välja töötada vahendeid, millega arvestatakse konkreetse tööstusharu, ärimudeli ja/või ettevõtja erivajadusi või -tingimusi. Need võivad olla näiteks lepingu tüüptingimused, mis on kohandatud konkreetse sektori nõuete suhtes, nt erilised kaitsemeetmed, kui töödeldakse delikaatseid isikuandmeid tervishoiusektoris, või teatavates kolmandates riikides levinud konkreetsete töötlemistoimingute nõuete suhtes, nt Euroopa äriühingute jaoks sisseostetavad teenused. Seda saab teha kas võttes vastu uusi lepingu tüüptingimuste kogumeid või lisades olemasolevatele tüüptingimustele täiendavaid kaitsemeetmeid, mis võivad olla tehnilised või korralduslikud või ärimudeliga seotud lahendused⁴⁴. Mõningate majandussektorite erivajadusi saab rahuldada ka siduvate kontsernisest eeskirjade abil, mida kohaldatakse ühise majandustegevusega tegelevate ettevõtjate rühma suhtes, nt reisisektoris. Isikuandmete rahvusvahelisele edastamisele volitatud töötajate vahel aitaks kaasa töötajatevahelise lepingu tüüptingimuste ja/või töötajatele mõeldud siduvate kontsernisest eeskirjade väljatöötamine. Lõpetuseks pakuvad uued isikuandmete edastamise mehhanismid, nagu näiteks heakskiidetud toimimisjuhendid ja akrediteeritud sertifitseerimine kolmanda isiku poolt, ettevõtjatele võimaluse võtta isikuandmete rahvusvaheliseks edastamiseks kasutusele individuaalsed lahendused, kaotamata samal ajal näiteks privaatsusmürgisest tulenevaid konkurentsieeliseid. Mõningaid neist vahenditest saab kujundada edastusepõhise mehhanismina või osana üldisemast vahendist, millega saab näidata kõigist isikuandmete kaitse üldmääruse sätetest kinnipidamist, nagu näiteks heakskiidetud toimimisjuhendi puhul.

⁴⁴ Vt isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktid c ja d ning põhjendus 109, milles on selgitatud, et heakskiidetud standardklauslite kohandamine on võimalik, tingimusel et see ei lähe otseselt ega kaudselt vastuollu nende klauslitega ega piira üksikisikute põhiõigusi ja -vabadusi.

Komisjon töötab koos ettevõtjate, kodanikuühiskonna ja andmekaitseasutustega selle nimel, et isikuandmete kaitse üldmääruse erinevate võimaluste potentsiaal andmete rahvusvahelise edastamise hõlbustamiseks täielikult ära kasutada. Andmekaitsereformi rakendamise raames sidusrühmadega toimuva dialoogi käigus tehakse kindlaks valdkonnad, kus tuleks sellega seoses esmajärjekorras meetmeid võtta. Selleks tuleb võib-olla lõpule viia juba alustatud tegevusi, näiteks töötajatevahelise lepingu tüüptingimuste koostamine koostöös artikli 29 alusel asutatud tööühmaga (mille asemele astub 2018. aastal Euroopa Andmekaitsekoostööühendus)⁴⁵. See võib hõlmata ELi vastavussüsteemile uute komponentide väljatöötamist, näiteks sel teel, et komisjon määratleb nõuded ja tehnilised standardid sertifitseerimismehhanismide loomiseks ja toimimiseks, kaasa arvatud andmete rahvusvahelise edastamisega seotud aspektides⁴⁶. Mõningate meetmete puhul võib abiks olla ka rahvusvaheline koostöö, eeskätt organisatsioonidega, kes on välja töötanud sarnaseid andmete edastamise mehhanisme. Näiteks võiks uurida võimalusi, kuidas lähendada ELi õigusel sätestatud siduvaid kontserniseseid eeskirju ning Aasia ja Vaikse ookeani piirkonna riikide majanduskoostöö foorumi (APEC) väljatöötatud piiriüleseid privaatsuseeskirju⁴⁷ nii mõlema süsteemi puhul kohaldatavate nõuete kui ka kohaldamisprotsessi osas. Sel teel õnnestuks edendada rangete andmekaitseõuete kehtestamist kogu maailmas ja ületada erinevusi lähenemisviisides privaatsusele ja isikuandmete kaitsele, aidata ettevõtjatel erinevate süsteemidega hakkama saada ja kujundada poliitika, mis on eri süsteemidega vastavuses.

Komisjon:

- töötab koos sidusrühmadega, et arendada alternatiivseid isikuandmete edastamise mehhanisme, mis on kohandatud vastavalt konkreetse tööstusharu, ärimudeli ja/või ettevõtja erivajadustele või -tingimustele.

3.3 Isikuandmete kaitseks tehtav rahvusvaheline koostöö

3.3.1. Andmekaitsenormide kasutamise edendamine mitmepoolsete õigusaktide ja foorumite abil

ELi andmekaitsealane õigusraamistik on sageli olnud eeskujuks kolmandatele riikidele, kes selles valdkonnas oma õigusakte välja töötavad. EL jätkab nii kahepoolset kui ka mitmepoolset aktiivset suhtlemist oma rahvusvaheliste partneritega, et soodustada õigusnormide lähenemist, edendades rangeid ja koostalitlusvõimelisi isikuandmete kaitse standardeid kõikjal maailmas. See aitab kaasa üksikisikute õiguste tõhusamale kaitsele ja vähendab samal ajal takistusi piiriüleste andmevoogude teel, mis on vabakaubanduse oluline osa.

⁴⁵ Praegu ei ole välja töötatud lepingu tüüptingimusi, mida saaks kasutada ELi volitatud töötajate ja ELi-välise volitatud töötajate vahel.

⁴⁶ Isikuandmete kaitse üldmääruse artikli 43 lõiked 8 ja 9.

⁴⁷ Vt APECi/ELi 2014. aasta ühisdokument, milles käsitletakse ELi siduvate kontserniseseid eeskirjade ja APECi piiriüleste privaatsuseeskirjade süsteemi ülesehitust ning võrreldakse mõlema süsteemi vastavus- ja sertifitseerimisnõudeid: http://www.apec.org/~media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf (inglise keeles).

Eeskätt julgustab komisjon kolmandaid riike ühinema Euroopa Nõukogu konventsiooniga 108 ja selle lisaprotokolliga⁴⁸. Konventsioon 108 on ühinemiseks avatud riikidele, kes ei ole Euroopa Nõukogu liikmed, ning selle on juba ratifitseerinud 50 riiki, sealhulgas Aafrika ja Lõuna-Ameerika riigid⁴⁹. Ühtlasi on see ainus siduv mitmepoolne õigusakt andmekaitse valdkonnas. Konventsioon 108 on praegu läbivaatamisel ja komisjon toetab aktiivselt ajakohastatud teksti kiiret vastuvõtmist, et ka EL saaks konventsiooniga ühineda. Konventsiooni uuendatud tekstis kajastuvad samad põhimõtted, mis on sätestatud ELi uutes andmekaitse normides, seega aitab see kaasa liikumisele rangete andmekaitse õuete suunas.

2017. aasta G20 kohtumine annab ELile veel ühe võimaluse koguda poolehoidu põhimõttele, et ranged andmekaitse nõuded kuuluvad vältimatult globaalse infoühiskonna edasise arengu juurde, et see ühiskond oleks võimeline edendama innovatsiooni, majanduskasvu ja sotsiaalset heaolu⁵⁰.

Komisjon loodab sisse seada positiivsed suhted ka uute oluliste toimijatega, nagu näiteks privaatsusõigusega tegelev ÜRO eriraportöör,⁵¹ ning edasi arendada juba toimivaid suhteid piirkondlike organisatsioonidega nagu APEC, et kõikjal maailmas edendada püüdeid austada isikute õigust privaatsusele ja isikuandmete kaitsele.

Osana ulatuslikumatest jõupingutustest suurendada teadlikkust privaatsuse valdkonnas ja parandada andmekaitsealaseid tagatiseid rahvusvaheliselt, kiitis Euroopa Komisjon 15. novembril 2016 partnerluse rahastamisvahendist heaks projekti, mille eesmärk on tugevdada koostööd partnerriikidega selles valdkonnas⁵². Projekti raames rahastatakse muu hulgas selliseid tegevusi nagu koolitused ja teadlikkuse tõstmine. EL omakorda saab reformi rakendamise käigus õppida teiste süsteemide tavade ja kogemuste vahetamisest seoses privaatsuse kaitse valdkonnas esilekerkivate uute teemade ning õiguslike või tehniliste lahendustega näiteks sellistes küsimustes nagu õigusnormide täitmise tagamine, vastavuse tagamise vahendid (nt sertifitseerimismehhanismid, privaatsuse alased mõjuhinnangud) või teatavate kindlat liiki andmete (nt laste andmete) kaitse.

3.3.2. Koostöö õigusnormide täitmise tagamisel

Koostöö kolmandate riikide asjaomaste privaatsusnormide täitmise tagamise ja järelevalveasutustega omandab järjest suuremat rolli, arvestades et globaalse haardega hargmised äriühingud töötlevad tohutu suuri isikuandmete hulki paljudes riikides. Sageli mõjutavad andmekaitse normide ja isikuandmetega seotud rikkumised inimesi korraga rohkem kui ühes riigis. Sel juhul võiks üksikisikute kaitse olla tõhusam, kui järelevalveasutused

⁴⁸ 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 liikumist üle piiri käsitlev 2001. aasta lisaprotokoll (ETS nr 181).

⁴⁹ Konventsiooni on ratifitseerinud Mauritius, Senegal ja Uruguay. Konventsiooniga on kutsutud ühinema ka Cabo Verde Vabariik, Maroko ja Tuneesia.

⁵⁰ Vt ka OECD ministrite deklaratsioon digitaal-majanduse kohta: innovatsioon, majanduskasv ja sotsiaalne heaolu („Cancuni deklaratsioon”), 23. juuni 2016.

⁵¹ Vt <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>.

⁵² Komisjoni rakendusotsus C(2016)7198, millega kinnitatakse partnerluse rahastamisvahendi 2016. aasta tegevuskava teine etapp.

tegutseksid ühiselt. Ettevõtjate jaoks oleks samas parem kui õiguskeskkond oleks selgem ning ühtseid tõlgendamisvahendeid ja õigusnormide täitmise tagamise tavadid kujundataks globaalsel tasandil.

Andmevoogude piirideta ja ühendatud maailmas on seetõttu aeg intensiivistada koostööd õigusnormide täitmise tagajate vahel⁵³. EL on valmis selleks oma panuse andma. Nagu eespool märgitud, on isikuandmete kaitse üldmäärusega antud komisjonile volitused töötada välja rahvusvahelised koostöömehhanismid, millega hõlbustada isikuandmete kaitset käsitlevate õigusaktide tõhusa täitmise tagamist, sealhulgas vastastikuse abi osutamise teel. Sellega seoses tuleks uurida võimalusi töötada välja koostöö raamleping ELi andmekaitseasutuste ja teatavate kolmandate riikide õigusnormide täitmise tagamise asutuste vahel, tuginedes muu hulgas komisjoni kogemustele õigusnormide täitmise tagamisel teistes valdkondades, nagu näiteks konkurents ja tarbijakaitse.

Komisjon:

- toetab Euroopa Nõukogu konventsiooni 108 ajakohastatud teksti kiiret vastuvõtmist, et ka EL saaks konventsiooniga ühineda, ja julgustab kolmandaid riike konventsiooniga ühinema;
- kasutab selliseid mitmepoolseid foorumeid nagu ÜRO, G20 ja APEC, et edendada kõikjal maailmas austust isikuandmete kaitse vastu;
- töötab koos oluliste rahvusvaheliste partneritega välja rahvusvahelised koostöömehhanismid, millega hõlbustada isikuandmete kaitset käsitlevate õigusaktide tõhusa täitmise tagamist.

4. TÕHUSAM KOOSTÖÖ ÕIGUSKAITSE VALDKONNAS TUGEVADE ANDMEKAITSEMEETMETEGA

Isikuandmete vahetamine on süütegude tõkestamiseks, uurimiseks ja isikute nende eest vastutusele võtmiseks hädavajalik. Kuna kuritegevus ei peatu riigipiiridel, on ühendatud maailmas isikuandmete kiire vahetamine eduka õiguskaitsealase koostöö ja kuritegevusevastase võitluse oluline osa. Isikuandmete edastamist peavad toetama tugevad andmekaitsemeetmed. See aitab luua õiguskaitseasutuste vastastikust usaldust ning suurendada õiguskindlust andmete kogumisel ja/või vahetamisel.

⁵³ Olemas on selline võrgustik nagu 2010. aastal OECD egiidi all asutatud ülemaailmne privaatsuse kaitse tagamise võrgustik (*Global Privacy Enforcement Network – GPEN*). See on privaatsusnormide täitmise tagamise asutuste mitteametlik võrgustik, milles osalevad ELi andmekaitseasutused ning mille ülesanded on muu hulgas õiguskaitsealane koostöö, parimate tavade jagamine piiriüleste probleemide lahendamiseks ning ühiste õigusnormide täitmise tagamise algatuste ja teadlikkuse tõstmise kampaaniate toetamine. Võrgustikus osalemine ei loo osalejatele uusi õiguslikult siduvaid kohustusi ja see tegeleb peamiselt koostöö hõlbustamisega erasektorit reguleerivate privaatsusnormide täitmise tagamise valdkonnas. Vt <https://privacyenforcement.net/>.

Andmete rahvusvahelist edastamist käsitlevad normid, mis on sätestatud politseidirektiivis, reguleerivad nii isikuandmete vahetamist ELi ja ELi-väliste õiguskaitseasutuste vahel kui ka, teatavatel juhtudel, andmete edastamist õiguskaitseasutustelt muudele üksustele. Direktiiviga on ette nähtud võimalus teha kaitse piisavuse otsuseid kriminaalõiguse valdkonnas. Komisjon toetab selle võimaluse kasutamist nõuetele vastavate kolmandate riikide puhul, eeskätt selliste riikide puhul, kellega tuleb teha tihedat ja kiiret koostööd kuritegevuse- ja terrorismivastases võitluses ning kellega juba vahetatakse isikuandmeid suures ulatuses. Eeltoodule tuginedes alustab komisjon esmajärjekorras arutelusid kaitse piisavuse üle kolmandate riikidega, kes on selles ettevõtmises olulised partnerid.

Teisalt on 2016. aasta detsembris sõlmitud ELi-USA andmekaitsealane raamleping⁵⁴ suurepärase näide sellest, kuidas saab tõhustada õiguskaitseasutuste koostööd tähtsa rahvusvahelise partneriga, kui lepatakse kokku rangetes andmekaitsemeetmetes. Kuna raamleping täiendab automaatselt kehtivaid õigusakte, millele andmevahetus tugineb (eelkõige kahepoolseid lepinguid nii ELi kui ka liikmesriikide tasandil), saavad inimesed raamlepingust kohe otsest kasu ja teabevahetust hõlbustades tugevdab see koostööd õiguskaitseasutuste vahel. Samuti kujutab raamleping endast alust kõigile tulevastele andmete edastamist käsitlevatele kokkulepetele Ameerika Ühendriikidega, mis tähendab, et edaspidi kaob vajadus korduvalt läbi rääkida samade kaitsemeetmete üle. Raamleping on esimene kahepoolne rahvusvaheline leping, mis sisaldab põhjalikku loetelu andmekaitsealastest õigustest ja kohustustest, mis on kooskõlas ELi õigusega. Seetõttu võib selle aluseks võtta sarnaste lepingute läbirääkimisel kolmandate riikidega mitte ainult politsei- ja õigusala koostöö valdkonnas, vaid ka muudes valdkondades, kus avaliku sektori asutused tagavad õigusaktide täitmist (nt konkurentsipoliitika, tarbijakaitse). See hõlmaks nii valitsustevahelist andmevahetust kui ka andmete edastamist eraettevõtete ja õiguskaitseasutuste vahel. Samuti lihtsustaks see liidul kokkulepete sõlmimist andmete edastamise kohta asjaomaste ELi ametite (eelkõige Europol ja Eurojust) ning kolmandate riikide vahel⁵⁵. Komisjon uurib seega võimalusi sõlmida sarnaseid raamlepinguid oluliste partneritega õiguskaitse valdkonnas.

Lisaks sellele on politseidirektiiviga ette nähtud võimalus, et teatavatel asjaoludel ja rangeid kaitsemeetmeid kohaldades võib ELi õiguskaitseasutus esitada teabenõude otse kolmanda riigi eraettevõttele ja edastada selles teabenõudes isikuandmeid (tavaliselt nimi või IP-aadress)⁵⁶. Seevastu isikuandmete kaitse üldmääruses on reguleeritud juhtumid, kui ELi eraettevõtte edastab isikuandmeid kolmanda riigi õiguskaitseasutusele viimase nõudel – isikuandmete edastamine väljapoole ELi on lubatud ainult kindlatel tingimustel, nt

⁵⁴ ELi ja USA vaheline isikuandmete kaitse kokkulepe, milles käsitletakse kriminaalasjades tehtava politsei- ja õigusala koostöö raames süütegude, sealhulgas terrorismi tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise eesmärgil edastatavate ja töödeldavate isikuandmete kaitset: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf (andmekaitsealane raamleping)

⁵⁵ Operatiivkoostöö kokkulepete sõlmimine Europoli ja Eurojustiga on olnud üks kriteeriume viisanõude kaotamise teemalistes dialoogides teatavate kolmandate riikidega, sealhulgas käimasolevas dialoogis Türgiga.

⁵⁶ Vt politseidirektiivi artikkel 39 ja põhjendus 73.

rahvusvahelise lepingu alusel või juhul, kui andmete avaldamine on vajalik kaaluka avaliku huvi tõttu, mis on sätestatud liidu või liikmesriigi õiguses⁵⁷.

Seda koostööd, mis on omandanud keskse koha kuritegevuse ja terrorismi edukas uurimises ning isikute vastutusele võtmises, on esile tõstetud nõukogu järeldustes küberruumi käsitleva kriminaalõigussüsteemi parandamise kohta. Nõukogu kutsub komisjoni võtma ELi ühisel lähenemisviisil põhinevaid konkreetseid meetmeid, et parandada koostööd teenusepakkujatega, tõhustada vastastikuse õigusabi pakkumist ning pakkuda välja lahendusi õiguskaitsepädevuse kindlaks tegemiseks küberruumis⁵⁸. Need meetmed hõlmavad andmete vahetamist nii ELis asuvate õiguskaitseasutuste ja teenusepakkujate vahel kui ka ELi-väliste asutuste ja ettevõtete ja ettevõtete. Komisjon esitab 2017. aasta juunis võimalikud variandid, mis käsitlevad juurdepääsu elektroonilistele tõenditele, võttes arvesse vajadust kiire ja usaldusväärse koostöö järele, mida toetavad politseidirektiivi ja isikuandmete kaitse üldmääruse ranged andmekaitse normid, nii ELi-sisestes olukordades kui ka rahvusvahelise andmevahetuse puhul.

Lõpetuseks hindab komisjon kooskõlas Europoli uue õigusliku alusega Europoli ja kolmandate osapoolte poolt nõukogu otsuse 2009/371/JSK kohaselt sõlmitud operatiivkoostöö lepingute sätteid, sealhulgas andmekaitset käsitlevaid sätteid⁵⁹. Lisaks sellele, nagu on märgitud 2015. aasta Euroopa julgeoleku tegevuskavas, arvestatakse liidu tulevases lähenemisviisis, mis käsitleb broneeringuinfo vahetamist ELi mittekuuluvate riikidega, vajadust kohaldada järjepidevaid nõudeid ja põhiõiguste kaitse spetsiifilisi sätteid. Komisjon töötab kolmandate riikidega broneeringuinfo vahetamise õiguslikult põhjendatud ja jätkusuutlike lahenduste kallal. Üks võimalus võiks näiteks olla sellise broneeringuinfo näidislepingu koostamine, milles määratakse kindlaks nõuded, mis kolmandatel riikidel tuleb täita, et saada ELilt broneeringuinfot. Tuleb siiski silmas pidada, et selle valdkonna reguleerimisel tuleb igal juhul arvesse võtta Euroopa Liidu Kohtus koostatavat arvamust kavandatava ELi-Kanada broneeringuinfo lepingu kohta⁶⁰.

⁵⁷ Vt isikuandmete kaitse üldmääruse artikkel 48 ja põhjendus 115.

⁵⁸ Euroopa Liidu nõukogu järeldused küberruumi käsitleva kriminaalõigussüsteemi parandamise kohta, 9. juuni 2016: <http://data.consilium.europa.eu/doc/document/ST-10007-2016-INIT/et/pdf>. Komisjonile on (pärast 2016. aasta detsembris nõukogule esitatud vahearuanne) tehtud ülesandeks esitada neid küsimusi käsitleva töö tulemused nõukogule 2017. aasta juuniks.

⁵⁹ Vt Euroopa Parlamendi ja nõukogu 11. mai 2016. aasta määruse (EL) 2016/794 (mis käsitleb Euroopa Liidu Õiguskaitsekoostöö Ametit (Europol) ning millega asendatakse ja tunnistatakse kehtetuks nõukogu otsused 2009/371/JSK, 2009/934/JSK, 2009/935/JSK, 2009/936/JSK ja 2009/968/JSK) artikli 25 lõige 4, ELT L 135, 24.5.2016 (lk 53–114). Komisjon peab 14. juuniks 2021 esitama hindamisaruande Europoli koostöölepingute kohta, mis on sõlmitud enne 1. maid 2017.

⁶⁰ Kohtu arvamus 2014. aasta ELi-Kanada broneeringuinfo lepingu eelnõu kohta, mida taotles kohtult Euroopa Parlament (arvamus 1/15). Kohtul paluti hinnata, kas lepingu eelnõu on kooskõlas ELi põhiõiguste hartaga.

TÕHUSAM KOOSTÖÖ ÕIGUSKAITSE VALDKONNAS TUGEVATE ANDMEKAITSEMEETMETEGA

Komisjon:

- toetab politseidirektiivi kohaselt kaitse piisavuse otsuste tegemise võimalust nõuetele vastavate kolmandate riikide puhul;
- toetab lepingute läbirääkimist õiguskaitse valdkonnas oluliste rahvusvaheliste partneritega, võttes eeskujuks USAga sõlmitud andmekaitsealase raamlepingu;
- tuginedes nõukogu järeldustele küberruumi käsitleva kriminaalõigussüsteemi parandamise kohta, jätkab tööd elektrooniliste tõendite piiriülese vahetamise hõlbustamiseks kooskõlas andmekaitse normidega.

5. KOKKUVÕTE

Isikuandmete kaitsmine ja vahetamine ei ole üksteist välistavad tegevused. Tugev andmekaitse süsteem hõlbustab andmevoogude liikumist, kuna tarbijad usaldavad rohkem selliseid ettevõtteid, kes hoolivad oma klientide andmete turvalisusest. Ranged andmekaitse nõuded muutuvad seega globaalses digitaalajanduses eeliseks. Sama kehtib õiguskaitsealase koostöö kohta – privaatsuse kaitse meetmed kuuluvad lahutamatu osana kuritegevusevastaseks võitluseks vajaliku tõhusa ja kiire teabevahetuse juurde, mis põhineb vastastikusel usaldusel ja õiguskindlusel.

EL on oma andmekaitse normide reformi lõpule viinud ja peaks nüüd kolmandate riikidega aktiivselt sel teemal suhtlema. EL peaks nii kahepoolset kui ka mitmepoolset tasandil püüdlema selle poole, et andmekaitse põhimõtted ühtlustuksid rahvusvaheliselt paremuse suunas. See on kodanike, aga ka ettevõtete huvides ja neile kasulik. Uus andmekaitsealane seadusandlik raamistik annab ELile vajalikud ja sobivad tööriistad nende eesmärkide saavutamiseks. Käesolevas teatises esitatud strateegilisele lähenemisviisile tuginedes hakkab komisjon aktiivselt suhtlema oluliste kolmandate riikidega, et uurida võimalusi kaitse piisavuse otsuste vastu võtmiseks, alustades Jaapani ja Koreaga 2017. aastal ning pidades silmas õigusnormide lähendamist ELi nõuetele ja kaubandussuhete lihtsustamist. Samal ajal kasutab EL täiel määral ära andmete edastamise alternatiivsete vahendite võimalused, et kaitsta isikute õigusi andmete kaitsele ja toetada ettevõtjaid, kui andmeid edastatakse riikidesse, mille siseriiklikus õiguses ei ole tagatud isikuandmete kaitse piisav tase. Neid vahendeid tuleks kasutada ka selleks, et veelgi hõlbustada koostööd ELi järelevalve- ja õiguskaitseasutuste ning nende rahvusvaheliste partnerite vahel. Komisjon tagab ELi andmekaitsepoliitika sise- ja välismõõtme sidususe ning edendab tugevat andmekaitset rahvusvahelisel tasandil, et parandada õiguskaitsealast koostööd, panustada vabakaubandusse ja kujundada välja ranged isikuandmete kaitse nõuded kogu maailmas.