Arvamus 5/2023 Euroopa Komisjoni rakendusotsuse eelnõu kohta, mis käsitleb isikuandmete piisavat kaitset ELi-USA andmekaitseraamistiku alusel

Vastu võetud 28. veebruaril 2023

Kokkuvõte

13. detsembril 2022 avaldas Euroopa Komisjon kaitse piisavuse otsuse eelnõu (edaspidi „otsuse eelnõu“), mille lisad moodustavad Atlandi-ülese isikuandmete vahetamise uue raamistiku, ELi-USA andmekaitseraamistiku (edaspidi „andmekaitseraamistik“), millega asendatakse varasem USA andmekaitseraamistik Privacy Shield, mille Euroopa Liidu Kohus 16. juulil 2020 kohtuotsuses Schrems II kehtetuks tunnistas. Andmekaitseraamistiku põhielement on ELi-USA andmekaitseraamistiku põhimõtted, sealhulgas täiendavad põhimõtted (edaspidi üheskoos „andmekaitseraamistiku põhimõtted“).

Kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679[1] (edaspidi „isikuandmete kaitse üldmäärus“) artikli 70 lõike 1 punktiga s palus komisjon Euroopa Andmekaitsenõukogul (edaspidi „andmekaitsenõukogu“) esitada otsuse eelnõu kohta arvamus.

Otsuse eelnõu läbivaatamisel hindas andmekaitsenõukogu USAs pakutava kaitse taseme piisavust. Andmekaitsenõukogu hindas nii kaubanduslikke aspekte kui ka EList edastatud isikuandmetele juurdepääsu ja nende andmete kasutamist USA avaliku sektori asutuste poolt.

Andmekaitsenõukogu võttis arvesse nii isikuandmete kaitse üldmääruses kehtestatud kohaldatavat ELi andmekaitsealast õigusraamistikku kui ka Euroopa Liidu põhiõiguste harta artiklites 7 ja 8 ning Euroopa inimõiguste konventsiooni artiklis 8 sätestatud põhiõigusi eraelu austamisele ja andmekaitsele. Samuti võttis andmekaitsenõukogu arvesse harta artiklis 47 sätestatud õigust tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele ning eri põhiõigustega seotud kohtupraktikat.

Peale selle kaalus andmekaitsenõukogu nõudeid, mis on sätestatud viimase vastuvõetud kaitse piisavuse viitedokumendis[2].

Andmekaitsenõukogu peamine eesmärk on esitada komisjonile arvamus nendele isikutele pakutava kaitse taseme piisavuse kohta, kelle isikuandmeid USAsse edastatakse. Oluline on tähele panna, et andmekaitsenõukogu ei eelda, et USA andmekaitseraamistik järgib Euroopa andmekaitsealaseid õigusakte.

Andmekaitsenõukogu tuletab meelde, et isikuandmete kaitse üldmääruse artikli 45 ja Euroopa Liidu Kohtu praktika kohaselt peab kolmanda riigi õigusaktidega andmesubjektidele tagatud kaitse tase selleks, et seda peetaks piisavaks, sisuliselt vastama ELis tagatud kaitse tasemele.

1.1. Andmekaitse üldised aspektid

Andmekaitseraamistikuga on ette nähtud, et mõnikord võivad raamistikuga hõlmatud organisatsioonid järgida andmekaitseraamistiku põhimõtteid piiratud ulatuses (näiteks sel määral, mis on vajalik kohtu määruse täitmiseks või avalikes huvides). Selleks et nende erandite mõju andmesubjektide kaitse tasemele paremini kindlaks teha, soovitab andmekaitsenõukogu komisjonil selgitada otsuse eelnõus erandite ulatust, sealhulgas USA õiguse alusel kohaldatavaid kaitsemeetmeid.

[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 1–88).

[2] Artikli 29 töörühm, kaitse piisavuse viitedokument, WP 254 rev. 01, 28. november 2017 (viimati läbi vaadatud ja vastu võetud 6. veebruaril 2018), mille andmekaitsenõukogu kinnitas 25. mail 2018 (edaspidi „kaitse piisavuse viitedokument“).

Andmekaitsenõukogu märgib, et lisade ülesehituse ja nende nummerduse tõttu on suhteliselt keeruline teavet leida ja sellele tugineda. See suurendab veelgi uue raamistiku üldist keerukat esitlust – raamistiku lisadesse on koondatud erineva õigusliku kaaluga dokumendid – ja selle tulemusel ei pruugi andmesubjektid, andmekaitseraamistikuga hõlmatud organisatsioonid ja ELi andmekaitseasutused andmekaitseraamistiku põhimõtetest hästi aru saada. Ühtlasi rõhutab andmekaitsenõukogu, et andmekaitseraamistikus tuleks kasutada terminoloogiat järjepidevalt. Samuti puudub mõne olulise termini määratlus[3].

Andmekaitsenõukogu tunneb heameelt ajakohastuste üle andmekaitseraamistiku põhimõtetes,[4] mis moodustavad andmekaitseraamistikuga hõlmatud organisatsioonide jaoks siduva õigusraamistiku, kuid märgib, et hoolimata mitmest muudatusest ja täiendavast selgitusest otsuse eelnõu põhjendustes ei ole andmekaitseraamistiku põhimõtted, mida raamistikuga hõlmatud organisatsioonid peavad järgima, võrreldes andmekaitseraamistiku Privacy Shield alusel kohaldatavate põhimõtetega (millel põhinesid artikli 29 alusel asutatud andmekaitse töörühma (edaspidi „artikli 29 töörühm“) ja andmekaitsenõukogu iga-aastased ühised läbivaatamised) sisuliselt muutunud. Samuti on andmekaitseraamistiku põhimõtted suures ulatuses samad kui andmekaitseraamistiku Privacy Shield eelnõus esitatud põhimõtted, millele tugines artikli 29 töörühma 2016. aasta arvamus[5]. Nende andmekaitseraamistiku põhimõtete puhul, mida sisuliselt ei muudetud, ei pea andmekaitsenõukogu vajalikuks kõiki artikli 29 töörühma varem esitatud märkusi korrata. Andmekaitsenõukogu otsustas keskenduda konkreetsetele aspektidele, mida ta õigusliku ja tehnoloogilise keskkonna arengut arvesse võttes praegu veelgi olulisemaks peab.

Näiteks märgib andmekaitsenõukogu, et jätkuvalt esinevad mõned murekohad, millele artikli 29 töörühm ja andmekaitsenõukogu on seoses andmekaitseraamistikuga Privacy Shield varem tähelepanu juhtinud. Eelkõige puudutavad need andmesubjektide õigusi (näiteks teatavad erandid seoses juurdepääsuõigusega ning vastuväite esitamise õiguse kasutamise aeg ja viisid), peamiste määratluste puudumist, ebaselgust seoses andmekaitseraamistiku põhimõtete kohaldamisega volitatud töötlejate suhtes ning laiaulatuslikku erandit avalikult kättesaadava teabe puhul[6].

Samuti soovib andmekaitsenõukogu korrata, et nendele isikutele tagatud kaitse taset, kelle andmeid edastatakse, ei tohi kahjustada edastatud andmete edasisaatmine nende algse saaja poolt[7]. Andmekaitsenõukogu kutsub veel kord komisjoni selgitama, et kaitsemeetmed, mille andmete algne saaja kolmandas riigis asuvale andmeimportijale kehtestab, peavad enne andmete andmekaitseraamistikus edasisaatmist olema tõhusad, võttes arvesse kolmanda riigi õigusakte.

Erilist tähelepanu nõuab automatiseeritud otsuste tegemise ja profiilianalüüsi valdkonna kiire areng, mis üha enam toimub tehisintellektipõhise tehnoloogia abil. Andmekaitsenõukogu tunneb heameelt komisjoni viidete üle konkreetsetele kaitsemeetmetele, mis on USA asjaomaste õigusaktidega eri valdkondades ette nähtud[8]. Üksikisikutele tagatud kaitse tase tundub aga erinevat, sõltuvalt sellest, milliseid sektoripõhiseid eeskirju (kui üldse) konkreetses olukorras kohaldatakse.

[3] Määratletud ei ole termineid „esindaja“ ja „volitatud töötleja“. Peale selle tuleb USA ametiasutustega veel arutada „personaliandmete“ mõistet.
[4] Näiteks selgitus, et kodeeritud andmed on isikuandmed.
[5] Artikli 29 töörühma arvamus 01/2016 ELi-USA andmekaitseraamistiku Privacy Shield piisavusotsuse eelnõu kohta (vastu võetud 13. aprillil 2016) (edaspidi „artikli 29 töörühma arvamus 01/2016“).
[6] ELi-USA andmekaitseraamistik Privacy Shield – kolmas iga-aastane ühine läbivaatamine, andmekaitsenõukogu 12. novembril 2019 vastu võetud aruanne, punkt 11.
[7] Isikuandmete kaitse üldmäärust käsitlev kaitse piisavuse viitedokument, punkt 3.A.9.
[8] Otsuse eelnõu põhjendus 35.

Andmekaitsenõukogu jääb oma seisukoha juurde, et vaja on erieeskirju automatiseeritud otsuste tegemise kohta, et tagada piisavad kaitsemeetmed, sealhulgas üksikisiku õigus teada kasutatavat loogikat, õigus otsus vaidlustada ja õigus otsesele isiklikule kontaktile.

Andmekaitsenõukogu tuletab meelde andmekaitseraamistiku üle tehtava tõhusa järelevalve ja raamistiku nõuete täitmise tagamise tähtsust ning leiab, et äärmiselt oluline on kontrollida sisulisematele nõuetele vastavust. Andmekaitsenõukogu jälgib neid aspekte hoolikalt, muu hulgas korrapäraste läbivaatamiste raames. Andmekaitsenõukogu võtab teadmiseks föderaalse kaubanduskomisjoni (edaspidi „FTC“)[9] ja transpordiministeeriumi[10] kirjades uuesti kinnitatud kohustused seoses nõuete täitmise tagamisega, näiteks kohustuse käsitada prioriteetsena andmekaitseraamistiku väidetavate rikkumiste uurimist.

Andmekaitsenõukogu märgib, et juhul, kui ELi andmesubjektide isikuandmete töötlemisel rikutakse andmekaitseraamistikku, on neil kasutada seitse õiguskaitsevahendit. Need õiguskaitsemehhanismid on samad kui endises andmekaitseraamistikus Privacy Shield sisalduvad mehhanismid, mille kohta artikli 29 töörühm on märkusi esitanud[11]. Andmekaitsenõukogu jälgib hoolikalt, muu hulgas korrapäraste läbivaatamiste raames, nende õiguskaitsemehhanismide tõhusust.

1.2. Juurdepääs Euroopa Liidust edastatud isikuandmetele ja nende kasutamine USAs asuvate avaliku sektori asutuste poolt

Euroopa Komisjon järeldab otsuse eelnõus, et „selliste üksikisikute põhiõiguste riivamine USA avaliku sektori asutuste poolt avalikes huvides ning eelkõige kriminaalõiguskaitse tagamise ja riikliku julgeoleku eesmärgil, kelle isikuandmeid ELi-USA andmekaitseraamistiku alusel liidust USAsse edastatakse, piirdub asjaomase seadusliku eesmärgi saavutamiseks rangelt vajalikuga ning tagatud on tõhus õiguskaitse selliste riivete vastu“[12].

Euroopa Komisjon tegi oma otsuse pärast seda, kui oli põhjalikult hinnanud korraldust (Executive Order) 14086 (edaspidi „EO 14086“), millega tõhustati USA signaaliluurealase tegevusega seotud kaitsemeetmeid. USA president andis korralduse EO 14086 välja 7. oktoobril 2022 pärast Euroopa Komisjoni ja USA valitsuse vahelisi läbirääkimisi, mis järgnesid eelmise kaitse piisavuse otsuse (Privacy Shield) kehtetuks tunnistamisele Euroopa Liidu Kohtu poolt.

Andmekaitsenõukogu pooldaks olukorda, kus mitte üksnes otsuse jõustumine, vaid ka selle vastuvõtmine sõltuvad sellest, et muu hulgas võtavad kõik USA luureasutused vastu ajakohastatud poliitika ja menetlused EO 14086 rakendamiseks. Andmekaitsenõukogu soovitab komisjonil hinnata seda ajakohastatud poliitikat ja neid menetlusi ning jagada seda hinnangut andmekaitsenõukoguga.

Seoses valitsuse juurdepääsuga USAsse edastatud isikuandmetele on andmekaitsenõukogu oma analüüsis keskendunud uue EO 14086 hindamisele, sest sisuliselt on selle eesmärk käsitleda ja heastada puudusi, mille Euroopa Liidu Kohus tuvastas kohtuotsuses Schrems II, kus kohus leidis, et eelmine kaitse piisavuse otsus on kehtetu.

Andmekaitsenõukogu tunnistab, et USA signaaliluurealase tegevuse õigusraamistikku on EO 14086 vastuvõtmisega muudetud, ja on seisukohal, et selles korralduses sisalduvate täiendavate kaitsemeetmete näol on tegemist olulise edasiminekuga. Korraldusega EO 14086 kehtestatakse USA signaaliluure õigusraamistikus vajalikkuse ja proportsionaalsuse põhimõtted ning nähakse juhul, kui EL

[9] Otsuse eelnõu IV lisa.
[10] Otsuse eelnõu V lisa.
[11] Vt eelkõige artikli 29 töörühma arvamus 01/2016, punkti 2.2.6 alapunkt a.
[12] Otsuse eelnõu põhjendus 195.

nimetatakse nõuetele vastavaks piirkondliku majandusintegratsiooni organisatsiooniks, ELi üksikisikutele ette uus õiguskaitsemehhanism. Andmekaitsenõukogu leiab, et võrreldes eelmise nn ombudsmani mehhanismiga andmekaitseraamistiku Privacy Shield alusel on uut õiguskaitsemehhanismi oluliselt täiustatud. Vastupidiselt varasemale õigusraamistikule, millega ei antud ELi üksikisikutele õigusi, nagu Euroopa Liidu Kohus sõnaselgelt märkis, antakse uue korraldusega EO 14086 kõnealused õigused ning nähakse ette rohkem kaitsemeetmeid andmekaitse apellatsioonikohtu sõltumatuse tagamiseks ja tõhusamad volitused rikkumiste suhtes kaitsemeetmete võtmiseks.

Võrreldes korralduses EO 14086 sisalduvaid täiendavaid kaitsemeetmeid nendega, mille andmekaitsenõukogu on sõnastanud Euroopa oluliste tagatistena kui Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu praktika põhjal koostatud standardina, tegi andmekaitsenõukogu oma hinnangus jätkuvalt kindlaks mitu küsimust, mida tuleb täiendavalt selgitada, millele tuleb tähelepanu pöörata või mis kujutavad murekohta. Need küsimused näitavad, et kuigi andmekaitsenõukogu arvamus põhines kohtuotsusel Schrems II, hõlmab tema hinnang paratamatult kaalutlusi, mis ulatuvad kohtuotsuses Schrems II tehtud konkreetsetest järeldustest kaugemale.

Andmekaitsenõukogu peab vajalikuks USA õigusraamistikus täiendavalt selgitada eelkõige andmete ajutist laiaulatuslikku kogumist ning (laiaulatuslikult) kogutud andmete edasist säilitamist ja levitamist.

Kuna sisulise samaväärsuse kontrollimisel ei kontrollita identsust ning kuna uues signaaliluure õigusraamistikus sisalduvaid kaitsemeetmeid on tugevdatud, on andmekaitsenõukogu tähelepanu ja tegevus suunatud peamiselt kaitsemeetmete kui terviku hindamisele, järgides igakülgset lähenemisviisi, mis hõlmab kaitsemeetmeid kogu töötlemistsükli jooksul, alates andmete kogumisest kuni nende levitamiseni, sealhulgas järelevalve ja õiguskaitse elemente.

Sellega seoses juhib andmekaitsenõukogu tähelepanu järgmistele järeldustele.

Kuigi andmekaitsenõukogu tunnistab, et korraldusega EO 14086 kehtestatakse signaaliluure õigusraamistikus vajalikkuse ja proportsionaalsuse põhimõtted, rõhutab ta vajadust hoolikalt jälgida nende muudatuste tegelikku mõju, sealhulgas vaadata läbi sisemenetlused ja tegevuspõhimõtted, millega korraldusega ette nähtud kaitsemeetmeid asutuste tasandil rakendatakse.

Samuti tunneb andmekaitsenõukogu heameelt asjaolu üle, et EO 14086 sisaldab loetelu konkreetsetest otstarvetest, milleks andmeid tohib või ei tohi koguda, ning märgib samas, et neid otstarbeid võib ajakohastada täiendavate – mitte tingimata avalike – eesmärkidega, võttes arvesse uusi riikliku julgeolekuga seotud tungivaid vajadusi.

Praeguse raamistiku puudusena on andmekaitsenõukogu kindlaks teinud eeskätt selle, et kui USA õigusraamistikuga on korralduse 12333 alusel lubatud andmete laiaulatuslik kogumine, siis ei sisalda see sõltumatu ametiasutuse eelneva heakskiidu nõuet, nagu nõutakse Euroopa Inimõiguste Kohtu hiljutise kohtupraktikaga, samuti ei ole sellega ette nähtud kohtu või samaväärse sõltumatu organi süstemaatilist sõltumatut järelhindamist. Mis puudutab eelnevat sõltumatut heakskiitu välisluure ja jälitustegevuse seaduse (Foreign Intelligence Surveillance Act, edaspidi „FISA“) paragrahvi 702 alusel, siis väljendab andmekaitsenõukogu kahetsust selle üle, et FISA kohus (FISA Court, edaspidi „FISC“) ei vaata selliste programmide kinnitamisel, millega lubatakse USA-väliste isikute andmete kogumine, läbi programmitaotluse vastavust korraldusele EO 14086, kuigi see korraldus on programmi ellu viivatele luureasutustele siduv. Andmekaitsenõukogu arvamuse kohaselt tuleks neid kõnealuses korralduses sisalduvaid täiendavaid kaitsemeetmeid siiski arvesse võtta, muu hulgas FISC poolt. Andmekaitsenõukogu tuletab meelde, et selle hindamisel, kuidas EO 14086 kohaseid kaitsemeetmeid rakendatakse ning kuidas neid kohaldatakse juhul, kui andmeid kogutakse FISA paragrahvi 702 ja

korralduse EO 12333 alusel, on väga kasulikud eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni (Privacy and Civil Liberties Oversight Board, edaspidi „PCLOB“) aruanded.

Mis puudutab õiguskaitsemehhanismi, siis tunnistab andmekaitsenõukogu, et seoses andmekaitse apellatsioonikohtu volitustega on tehtud suuri edusamme ja ombudsmaniga võrreldes on kohus palju sõltumatum. Samuti tunnustab andmekaitsenõukogu uue õiguskaitsemehhanismiga ette nähtud täiendavaid kaitsemeetmeid, näiteks erikaitsjate rolli, mis hõlmab kaebuse esitaja huvide kaitsmist, aga ka õiguskaitsemehhanismi läbivaatamist järelevalvekomisjoni poolt. Riikliku julgeoleku laadi ja korraldusega EO 14086 ette nähtud kaitsemeetmeid arvesse võttes valmistab andmekaitsenõukogule siiski muret andmekaitse apellatsioonikohtu standardvastuse (millega teavitatakse kaebuse esitajat, et hõlmatud rikkumisi ei tuvastatud või et tehti otsus asjakohaste kaitsemeetmete võtmise kohta) üldine kohaldamine koos asjaoluga, et seda ei saa edasi kaevata. Õiguskaitsemehhanismi tähtsust arvesse võttes kutsub andmekaitsenõukogu komisjoni selle mehhanismi toimimist hoolikalt jälgima.

Andmekaitsenõukogu eeldab, et komisjon täidab oma kohustust kaitse piisavuse otsus kiireloomulistel juhtudel peatada või kehtetuks tunnistada või seda muuta, eeskätt kui USA täitevvõim otsustab korralduses sisalduvaid kaitsemeetmeid piirata[13].

Üldiselt märgib andmekaitsenõukogu positiivselt ära olulised täiustused, mida korraldus võrreldes varasema õigusraamistikuga pakub, eelkõige vajalikkuse ja proportsionaalsuse põhimõtete kehtestamise ning individuaalse õiguskaitsemehhanismi ELi andmesubjektidele. Väljendatud muret ja vajalikke selgitusi arvestades soovitab andmekaitsenõukogu neid murekohti käsitleda ning komisjonil esitada nõutud selgitused, et tugevdada otsuse eelnõu aluseid ja tagada tulevastes ühistes läbivaatamistes selle uue õigusraamistiku konkreetse rakendamise hoolikas järelevalve, eriti sellega tagatud kaitsemeetmete üle.

[13] Otsuse eelnõu põhjendus 212.

Sisukord

Euroopa Andmekaitsenõukogu

Euroopa Andmekaitsenõukogu on võtnud vastu järgmise avalduse.

Võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta) (edaspidi „isikuandmete kaitse üldmäärus“)[1] artikli 70 lõike 1 punkti s,

võttes arvesse Euroopa Majanduspiirkonna (EMP) lepingut, eriti selle XI lisa ja protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018[2],

võttes arvesse oma töökorra artikleid 12 ja 22,

ON VASTU VÕTNUD JÄRGMISE ARVAMUSE:

1 SISSEJUHATUS

1.1 USA andmekaitseraamistik

1. Ameerika Ühendriikide (edaspidi „USA“) ja Euroopa Liidu (edaspidi „EL“) lähenemisviisid eraelu puutumatusele ja andmekaitsele on erinevad. Kui ELis on eraelu puutumatus ja andmekaitse Euroopa Liidu põhiõiguste harta artiklitega 7 ja 8 tagatud põhiõigused, siis USAs käsitletakse andmekaitset üldjuhul tarbijakaitse vaatenurgast. Sellest tulenevalt on reguleerimine USAs ja ELis erinev[3].

2. Erinevalt isikuandmete kaitse üldmääruse põhjal ELis järgitavast terviklikust lähenemisviisist puudub USAs föderaaltasandil üldine laiaulatuslik andmekaitseseadus. Pigem järgitakse USAs andmekaitse tagamisel valdkondlikke ja osariikide lähenemisviise. Näiteks on teatavad konkreetsed sektorid hõlmatud eriseadustega, nagu

    - ravikindlustuse teisaldatavuse ja vastutuse seadus (Health Insurance Portability and Accountability Act – HIPAA);[4]

[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) (EMPs kohaldatav tekst) (ELT L 119, 4.5.2016, lk 1).

[2] Käesolevas arvamuses esitatud viiteid liikmesriikidele tuleks mõista viidetena EMP liikmesriikidele.

[3] Vt ka Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 kohase Euroopa Komisjoni rakendusotsuse eelnõu (mis käsitleb isikuandmete kaitse piisavat taset ELi-USA andmekaitseraamistiku alusel) (avaldatud 13. detsembril 2022; edaspidi „otsuse eelnõu“) I lisa I jagu.

[4] 1996. aasta ravikindlustuse ja vastutuse seadus (HIPAA) on USA föderaalne seadus. Sellega kehtestatakse riiklikud normid patsientide tundlike terviseandmete kaitse kohta. HIPAA eesmärk on tagada üksikisikute terviseandmete piisav kaitse, võimaldades samal ajal terviseandmete edastamist kvaliteetsete tervishoiuteenuste osutamise ja edendamise eesmärgil. HIPAAga on reguleeritud terviseandmete kasutamine ja avalikustamine nende üksuste poolt, kelle suhtes kohaldatakse eraelu puutumatuse eeskirja. Samuti sisaldab see üksikisikute õigusi käsitlevaid norme, mis võimaldavad neil mõista ja kontrollida seda, kuidas nende terviseandmeid kasutatakse.

- internetis laste eraelu puutumatuse kaitse seadus (Children's Online Privacy Protection Act – COPPA);[5]
- Gramm-Leach-Bliley seadus (Gramm-Leach-Bliley Act – GLBA)[6].

3. Seoses valitsuse juurdepääsuga EList USAsse edastatud isikuandmetele kohaldatakse mitut erinevat õiguslikku alust, piirangut ja kaitsemeedet. Õiguslikud menetlused andmetele juurdepääsuks õiguskaitse eesmärkidel põhinevad otseselt USA põhiseadusel (neljas muudatus), asjaomastel seadustel ja menetlusõigusel või justiitsministeeriumi föderaalse või osariigi tasandi suunistel ja meetmetel. Teabele juurdepääs riikliku julgeoleku eesmärgil on reguleeritud mitme õigusaktiga, eelkõige välisluure ja jälitustegevuse seadusega (Foreign Intelligence Surveillance Act, edaspidi „FISA"), korraldusega 12333, hiljuti vastu võetud korraldusega 14086 ning justiitsministri (Attorney General) määrusega,[7] millega luuakse andmekaitse apellatsioonikohus.

4. 13. detsembril 2022 andis komisjon välja Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 kohase komisjoni rakendusotsuse eelnõu, mis käsitleb isikuandmete kaitse piisavat taset ELi-USA andmekaitseraamistiku alusel (edaspidi „otsuse eelnõu") ning mille lisas on esitatud ELi-USA andmekaitseraamistik (edaspidi „andmekaitseraamistik"). Eespool selgitatud põhjustel ei põhine otsuse eelnõu konkreetsel ja igakülgsel föderaalsel õigusraamistikul, vaid andmekaitseraamistikul.

5. Andmekaitseraamistik toimib järgmiselt: *„USA kaubandusministeerium (edaspidi „kaubandusministeerium") annab välja ELi-USA andmekaitseraamistiku põhimõtted, sealhulgas täiendavad põhimõtted (üheskoos „põhimõtted") ja põhimõtete I lisa (edaspidi „I lisa"), täites oma seadusest tulenevat volitust soodustada, edendada ja arendada rahvusvahelist kaubandust (15 U.S.C. § 1512)*"[8].

6. Andmekaitseraamistiku põhimõtted töötati välja koostöös Euroopa Komisjoni (edaspidi „komisjon"), tööstusharu ja teiste sidusrühmadega, et hõlbustada ELi ja USA vahelist kaubandust,[9] tagades samal ajal andmesubjektidele ELis pakutavaga sisuliselt samaväärse kaitsetaseme.

7. Andmekaitseraamistiku põhimõtteid kirjeldatakse kui andmekaitseraamistiku põhielementi. Ühelt poolt pakuvad need n-ö kasutusvalmis mehhanismi andmete edastamiseks EList USAsse. Teiselt poolt on EList USAsse edastatavatele isikuandmetele tagatud ELi õigusega nõutav kaitse.

---

https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; https://www.justice.gov/opcl/privacy-act-1974.

[5] COPPA põhieesmärk on anda vanematele kontroll selle üle, milliseid isikuandmeid lastelt suunatud veebisaitide ja veebiteenuste (sealhulgas mobiilirakenduste ja esemevõrguseadmete, näiteks nutimänguasjade) või laiemale publikule mõeldud veebisaitide haldajad nende alla 13aastastelt lastelt koguvad. COPPA kohaselt peavad need haldajad vanemaid teavitama ja hankima neilt kontrollitava nõusoleku. See kehtib ka välisriikide laste puhul, kui veebisaite või -teenuseid hallatakse USAs ja nende suhtes kohaldatakse COPPAt. Samal ajal kohaldatakse neid eeskirju ka välisriikide veebisaitide ja -teenuste suhtes, kui need on suunatud USAs asuvatele lastele. Vt https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions ja otsuse eelnõu IV lisa, lk 3.

[6] Gramm-Leach-Bliley seaduse üks eesmärk on kaitsta tarbijate eraelu puutumatust finantssektoris. GLBA alusel peavad finantsasutused selgitama klientidele oma teabe jagamise tavasid ja kehtestama kaitsemeetmed klientide andmete kaitsmiseks (näiteks FTC reguleeritud äriühingud FTC kaitsemeetmete eeskirja (Safeguards Rule) alusel), https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

[7] Justiitsministri korraldus nr 5517-2022, millega muudetakse USA justiitsministeeriumi määrusi, nagu on heaks kiidetud ja ette nähtud korraldusega EO 14086.

[8] Otsuse eelnõu I lisa I jagu.

[9] Samas.

8. Andmekaitseraamistikku kohaldatakse ainult nende USA organisatsioonide suhtes, kes on ise kinnitanud, et nad järgivad raamistiku nõudeid (edaspidi „andmekaitseraamistikuga hõlmatud organisatsioonid“). Praegu on see võimalik ainult juhul, kui nad jäävad föderaalse kaubanduskomisjoni (FTC) või transpordiministeeriumi jurisdiktsiooni alla. Edaspidi võidakse tulevasse lisasse kanda ka teisi täitevasutusi, kellel on pädevus andmekaitseraamistiku põhimõtete elluviimise üle järelevalvet teha.

9. Andmekaitseraamistiku põhimõtetes on selgitatud, et raamistiku tingimuste täitmise tagab i) FTC föderaalse kaubanduskomisjoni seaduse (edaspidi „FTC seadus“) paragrahvi 5 alusel (millega keelatakse äritegevuses kasutatavad või äritegevust mõjutavad ebaõiglased tavad ja pettus),[10] ii) transpordiministeerium õigusakti 49 U.S.C. § 41712 alusel (millega keelatakse lennuettevõtjatel või piletimüügiagentidel rakendada ebaõiglaseid või pettusel põhinevaid tavasid lennunduses lennupiletite müümiseks) või iii) tehakse seda muude seaduste või määruste alusel, millega selline tegevus on keelatud.

10. Andmekaitseraamistiku põhimõtetes on osutatud, et need ei mõjuta isikuandmete kaitse üldmääruse kohaldamist ega piira mis tahes kehtivaid eraelu puutumatust käsitlevaid kohustusi, mida USA õiguse alusel kohaldatakse.

1.2 Euroopa Andmekaitsenõukogu hinnangu ulatus

11. Otsuse eelnõu kajastab komisjoni hinnangut andmekaitseraamistikule, mis koostati USA valitsusega peetud arutelude tulemusel. Kooskõlas isikuandmete kaitse üldmääruse artikli 70 lõike 1 punktiga s esitab andmekaitsenõukogu arvamuse komisjoni järelduste kohta seoses kaitse taseme piisavusega kolmandas riigis ning esitab vajaduse korral ettepanekuid võimalike probleemide lahendamiseks.

12. Andmekaitsenõukogu tunneb heameelt ajakohastuste üle andmekaitseraamistiku põhimõtetes,[11] mis moodustavad andmekaitseraamistikuga hõlmatud organisatsioonide jaoks siduva õigusraamistiku. Andmekaitsenõukogu märgib aga, et sisuliselt on andmekaitseraamistiku põhimõtted jätkuvalt samad kui andmekaitseraamistiku Privacy Shield[12] alusel (millel põhinesid artikli 29 alusel asutatud andmekaitse töörühma (edaspidi „artikli 29 töörühm“) ja andmekaitsenõukogu iga-aastased ühised läbivaatamised). Samuti on andmekaitseraamistiku põhimõtted suures ulatuses samad kui andmekaitseraamistiku Privacy Shield eelnõus esitatud põhimõtted, millel põhines artikli 29 töörühma 2016. aasta arvamus[13] (edaspidi „artikli 29 töörühma arvamus 01/2016“). Nende andmekaitseraamistiku põhimõtete puhul, mida sisuliselt ei muudetud, ei pea andmekaitsenõukogu vajalikuks kõiki artikli 29 töörühma varem esitatud märkusi korrata. Andmekaitsenõukogu otsustas keskenduda konkreetsetele aspektidele, mida ta õigusliku ja tehnoloogilise keskkonna arengut arvesse võttes praegu veelgi olulisemaks peab.

[10] 15 U.S.C. § 45 (a).

[11] Näiteks selgitus, et kodeeritud andmete näol on tegemist isikuandmetega.

[12] Komisjoni 12. juuli 2016. aasta rakendusotsus (EL) 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (ELT L 207, 1.8.2016, lk 1).

[13] Artikli 29 töörühma arvamus 01/2016 ELi-USA andmekaitseraamistiku Privacy Shield piisavusotsuse eelnõu kohta (vastu võetud 13. aprillil 2016) (edaspidi „artikli 29 töörühma arvamus 01/2016“).

13. Peale selle hõlmab väga oluline osa analüüsist kooskõlas Euroopa Liidu Kohtu praktikaga[14] õiguskorda, millega on reguleeritud valitsuse juurdepääs USAsse edastatud isikuandmetele.

14. Oma hinnangus võttis andmekaitsenõukogu arvesse kohaldatavat Euroopa andmekaitseraamistikku, sealhulgas Euroopa Liidu põhiõiguste harta (edaspidi „harta“) artikleid 7, 8 ja 47, millega kaitstakse vastavalt õigust era- ja perekonnaelu austamisele, õigust isikuandmete kaitsele ning õigust tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, ning Euroopa inimõiguste konventsiooni artiklit 8, millega kaitstakse õigust era- ja perekonnaelu austamisele. Lisaks eespool kirjeldatule võttis andmekaitsenõukogu arvesse isikuandmete kaitse üldmääruse nõudeid, asjaomast kohtupraktikat ja andmekaitsenõukogu vastu võetud kaitse piisavuse viitedokumenti (edaspidi „isikuandmete kaitse üldmäärust käsitlev kaitse piisavuse viitedokument“)[15].

15. Selle tegevuse eesmärk on esitada komisjonile arvamus andmekaitseraamistikuga pakutava kaitsetaseme piisavuse hindamise kohta. Euroopa Liidu Kohus on mõistet „kaitse piisav tase“, mida kasutati juba direktiivi 95/46/EÜ alusel, edasi arendanud. Seepärast on oluline meelde tuletada norme, mille Euroopa Liidu Kohus kehtestas oma kohtuotsustes Schrems I[16] (millega tunnistati kehtetuks programm Safe Harbor) ja Schrems II[17] (millega tunnistati kehtetuks andmekaitseraamistik Privacy Shield).

16. Kohtuotsuses Schrems I sedastas Euroopa Liidu Kohus, et „kaitse tase“ kolmandas riigis peab olema „sisuliselt samaväärne“ sellega, mis on tagatud ELis, kuid „vahendid, mida kolmas riik sellega seoses niisuguse kaitsetaseme saavutamiseks kasutab, võivad olla erinevad nendest, mida liidus rakendatakse“[18]. Seepärast ei ole eesmärk kopeerida punkt-punktilt Euroopa õigusakte, vaid teha kindlaks uuritavate õigusaktide olulised ja kesksed nõuded. Piisavust on võimalik saavutada, kui omavahel kombineeritakse andmesubjektide õigused ja isikuandmete töötlejate või töötlemist kontrollivate isikute kohustused ning sõltumatute asutuste järelevalve. Samas on andmekaitse-eeskirjad tulemuslikud vaid siis, kui on võimalik tagada nende täitmine ja kui neist praktikas kinni peetakse. Seetõttu on kolmandasse riiki või rahvusvahelisele organisatsioonile edastatavate isikuandmete suhtes kohaldatavate normide sisu kõrval vaja vaadelda ka nende normide tulemuslikkuse tagamiseks kehtestatud süsteemi. Andmekaitse-eeskirjade tulemuslikkuse seisukohast on väga oluline, et olemas oleksid tõhusad mehhanismid nende eeskirjade täitmise tagamiseks[19].

17. Kohtuotsuses Schrems II leidis Euroopa Liidu Kohus, et õigusaktid, mille alusel USA luureasutustel on õigus USAsse edastatud isikuandmetele juurde pääseda (FISA paragrahv 702 / EO 12333) piiravad ebaproportsionaalsel määral ELi põhiõiguste harta artiklites 7 ja 8 sätestatud õigusi ega ole seega

[14] Eelkõige kohtuotsus, Euroopa Kohus, 6. oktoober 2015, Maximilian Schrems *vs.* Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650, ning kohtuotsus, Euroopa Kohus, 16. juuli 2020, Data Protection Commissioner *vs.* Facebook Ireland Limited ja Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[15] Artikli 29 töörühm, „Piisavuse võrdlusalus“, WP 254 rev. 01, 28. november 2017 (viimati läbi vaadatud ja vastu võetud 6. veebruaril 2018), mille andmekaitsenõukogu kinnitas 25. mail 2018 (edaspidi „isikuandmete kaitse üldmäärust käsitlev kaitse piisavuse viitedokument“).

[16] Kohtuotsus Schrems I, Euroopa Kohus, 6. oktoober 2015, Maximilian Schrems *vs.* Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650 (edaspidi „Euroopa Liidu Kohtu otsus Schrems I“).

[17] Kohtuotsus, Euroopa Kohus, 16. juuli 2020, Data Protection Commissioner *vs.* Facebook Ireland Limited ja Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (edaspidi „Euroopa Liidu Kohtu otsus Schrems II“).

[18] Euroopa Liidu Kohtu otsus Schrems I, punktid 73–74.

[19] Isikuandmete kaitse üldmäärust käsitlev kaitse piisavuse viitedokument, lk 2.

piiritletud viisil, mis vastaks ELi õiguses harta artikli 52 lõike 1 teises lauses ettenähtuga sisuliselt samaväärsetele nõuetele[20].

18. Peale selle märkis Euroopa Liidu Kohus, et varasemate õigusraamistikega ei pakutud harta artiklis 47 nõutavatega sisuliselt samaväärseid tagatisi, sest ombudsmani mehhanism ei korvanud asjaolu, et suunisega PPD-28 ega korraldusega EO 12333 ei tagatud USA-välistele isikutele tõhusat õiguskaitsevahendit[21]. Ombudsman ei olnud täitevvõimust sõltumatu ja tal puudus õigus võtta vastu USA luureasutustele siduvaid otsuseid[22].

19. Korralduses EO 14086, millega üldiselt asendati PPD-28, kehtestati USA õiguses kaks uut nõuet, mis kajastavad Euroopa Liidu Kohtu otsust Schrems II: ühelt poolt tohib signaaliluurega seotud tegevust ellu viia ainult sel määral, mil see on vajalik kinnitatud luureandmete prioriteetse kogumise soodustamiseks, ning üksnes selles ulatuses ja sel viisil, mis on proportsionaalne kinnitatud luureandmete prioriteetsusega, ning teiselt poolt kehtestati õiguskaitsemehhanism.

20. Käesolevas arvamuses hindab andmekaitsenõukogu eelkõige seda, mil määral on nii andmekaitseraamistikus kui ka hiljuti vastu võetud korralduses EO 14086 tõhusalt käsitletud järeldusi, mille Euroopa Liidu Kohus oma otsuses tegi.

1.3 Üldised märkused ja probleemid

1.3.1 Siseriikliku õiguse hindamine

21. Andmekaitsenõukogu mõistab, et otsuse eelnõus esitatud hinnang käsitleb andmekaitseraamistiku põhimõtteid. Sellest hoolimata sooviks andmekaitsenõukogu saada teatavat teavet USA õigusliku konteksti kohta, milles andmekaitseraamistikuga hõlmatud organisatsioonid tegutsevad. See võimaldaks paremini mõista andmekaitseraamistiku koostoimet USA õigusega. Näiteks on I lisa punktis 1[23] kirjas, et andmekaitseraamistiku põhimõtted ei piira „[---] Ameerika Ühendriikide õiguse alusel eraelu puutumatuse suhtes kohaldatavaid kohustusi“, kuid neid kohustusi ei ole kirjeldatud.

1.3.2 USA võetud rahvusvahelised kohustused

22. Vastavalt isikuandmete kaitse üldmääruse artikli 45 lõike 2 punktile c ja isikuandmete kaitse üldmäärust käsitlevale kaitse piisavuse viitedokumendile võtab komisjon kolmanda riigi kaitsetaseme piisavuse hindamisel muu hulgas arvesse ka kolmanda riigi võetud rahvusvahelisi kohustusi või muid kohustusi, mis tulenevad kolmanda riigi osalemisest mitmepoolsetes või piirkondlikes süsteemides, eelkõige seoses isikuandmete kaitsega, ning selliste kohustuste täitmist.

23. USA on osaline mitmes rahvusvahelises kokkuleppes, millega tagatakse õigus eraelu puutumatusele, näiteks kodaniku- ja poliitiliste õiguste rahvusvaheline pakt (artikkel 17), puuetega inimeste õiguste konventsioon (artikkel 22) ja lapse õiguste konventsioon (artikkel 16). Lisaks järgib USA OECD liikmena OECD eraelu puutumatuse raamistikku, eelkõige suuniseid isikuandmete kaitse ja piiriülese edastamise kohta. 14. detsembril 2022 võtsid OECD liikmete ja Euroopa Liidu ministrid ja kõrgetasemelised esindajad vastu OECD deklaratsiooni valitsuse juurdepääsu kohta erasektori üksuste valduses olevatele isikuandmetele. Samuti on USA küberkuritegevuse Budapesti konventsiooni osaline.

[20] Euroopa Liidu Kohtu otsus Schrems II, punktid 184–185.
[21] Euroopa Liidu Kohtu otsus Schrems II, punkt 192.
[22] Euroopa Liidu Kohtu otsus Schrems II, punkt 195.
[23] Otsuse eelnõu I lisa I jagu, viimane lause.

24. Lisaks osaleb USA Aasia ja Vaikse ookeani piirkonna riikide majanduskoostöö (edaspidi „APEC“) piiriüleste andmekaitse-eeskirjade süsteemis, mis on valitsuse toetatud andmekaitsealase sertifitseerimise süsteem, millega äriühingud saavad liituda, et tõendada rahvusvaheliselt tunnustatud andmekaitse-eeskirjade järgimist. APECi juhid on need andmekaitse-eeskirjad heaks kiitnud.

25. Andmekaitsenõukogu märgib ka, et USA osaleb vaatlejariigina Euroopa Nõukogu konventsiooni 108 nõuandekomitee töös.

26. Lisaks märgib andmekaitsenõukogu ja tunneb heameelt selle üle, et USA organid jätkasid osalemist hiljuti, 2021. aastal kehtestatud G7 andmekaitse- ja eraelu puutumatuse asutuste ümarlaua (edaspidi „G7 andmekaitseasutuste ümarlaud“) uues formaadis, mis koondab G7 riikide sõltumatuid andmekaitse ja eraelu puutumatuse järelevalveasutusi. Näiteks on nad toetanud G7 andmekaitseasutuste ümarlaua viimast, 8. septembril 2022 Saksamaal Bonnis vastu võetud kommünikeed,[24] milles keskenduti usaldusväärse andmete vaba liikumise algatuse „Data Free Flow with Trust“ kontseptsioonile.

1.3.3 USA andmekaitsealaste õigusaktide valdkonnas tehtud edusammud

27. Andmekaitsenõukogu märgib eelkõige ära USAs osariikide tasandil andmekaitsealastes õigusaktides toimunud arengu. Andmekaitsenõukogu tunneb heameelt andmekaitsealaste õigusaktide vastuvõtmise üle, mis on jõustunud või jõustuvad 2023. aastal viies osariigis (California, Colorado, Connecticut, Virginia ja Utah)[25].

28. Samuti märgib andmekaitsenõukogu, et paljudes teistes USA osariikides on juba käivitatud vastavad algatused täiendavate osariigi seaduste vastuvõtmiseks.

29. Peale selle avaldab andmekaitsenõukogu sõnaselgelt heameelt jõupingutuste üle seoses kahe erakonna algatusega võtta vastu föderaalne andmekaitseseadus (American Data Privacy and Protection Act – ADPPA).

1.3.4 Otsuse eelnõu kohaldamisala

30. Otsuse eelnõu artikli 1 kohaselt järeldab komisjon, et USA tagab piisava kaitsetaseme isikuandmetele, mida edastatakse EList Ameerika Ühendriikides asuvatele organisatsioonidele, kes on kantud nn andmekaitseloetellu, mida kooskõlas I lisa I jao punktiga 3 haldab ja mille teeb avalikult kättesaadavaks USA kaubandusministeerium[26].

---

[24] G7 andmekaitse- ja eraelu puutumatuse asutuste ümarlaud, „Usaldusväärse andmete vaba liikumise ja rahvusvahelise andmeruumi väljavaadete kohta teadmiste vahetamise edendamine“, 8. september 2022. https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

[25] California tarbijate andmekaitse seadus (2018, jõustus 1. jaanuaril 2020), California andmekaitseõiguste seadus (2020, jõustus täielikult 1. jaanuaril 2023), Colorado andmekaitseseadus (2021, jõustus 1. juulil 2023), Connecticuti andmekaitseseadus (2022, jõustus 1. juulil 2023), Virginia tarbijate andmekaitseseadus (2021, jõustus 1. jaanuaril 2023) ja Utah' tarbijate andmekaitse seadus (2022, jõustub 31. detsembril 2023).

[26] Otsuse eelnõu, lõppmärkused, artikkel 1, lk 57. Andmekaitsenõukogu mõistab, et otsuse eelnõus ei käsitleta andmete edastamist USAs asuvatele põhimõtete järgimist kinnitanud üksustele selliste üksuste poolt, kes asuvad väljaspool ELi, kuid kelle suhtes kohaldatakse isikuandmete kaitse üldmäärust selle määruse artikli 3 lõike 2 kohaselt.

31. Andmekaitseraamistikku saavad kasutada FTC või transpordiministeeriumi jurisdiktsiooni alla kuuluvad äriühingud. Veel juhitakse tähelepanu asjaolule, et tulevikus võivad lisanduda teised sarnaste volitustega täitevasutused[27].

1.3.5 Andmekaitseraamistiku põhimõtete järgimise kohustuse piirangud

32. I lisa I jao punktis 5 on sätestatud, et andmekaitseraamistiku põhimõtete järgimist andmekaitseraamistikuga hõlmatud organisatsioonide poolt võib piirata muu hulgas i) sel määral, mis on vajalik kohtu määruse täitmiseks või avalike huvide, õiguskaitse[28] või riikliku julgeolekuga seotud vajaduste täitmiseks[29] (sealhulgas juhul, kui seaduse või valitsuse määrusega kehtestatakse vastuolulised kohustused) ning ii) seaduse, kohtu määruse või valitsuse määrusega, millega antakse sõnaselged volitused, tingimusel et selliste volituste kasutamisel suudab andmekaitseraamistikuga hõlmatud organisatsioon tõendada, et andmekaitseraamistiku põhimõtete mittejärgimine tema poolt piirdub ulatusega, mis on vajalik selliste volitustega seotud ülekaaluka õigustatud huvi järgimiseks.

33. Tundmata kõiki USA seadusi nii föderaalsel kui ka osariikide tasandil, on andmekaitsenõukogul väga keeruline üksikasjalikult hinnata selles punktis loetletud erandite ulatust. Seepärast soovitab andmekaitsenõukogu komisjonil selgitada otsuse eelnõus erandite ulatust, sealhulgas USA õiguse alusel kohaldatavaid erandeid, et teha paremini kindlaks nende erandite mõju andmesubjektide kaitse tasemele. Ühtlasi rõhutab andmekaitsenõukogu, et komisjoni tuleks teavitada andmekaitseraamistiku põhimõtete järgimist mõjutavate seaduste või valitsuse määruste kohaldamisest ja vastuvõtmisest ning komisjon peaks seda jälgima.

1.3.6 Muudatused võrreldes andmekaitseraamistikuga Privacy Shield

34. Andmekaitsenõukogu tunneb heameelt kohtuotsuses Schrems II esitatud nõuete täitmiseks tehtud jõupingutuste üle. Sellest hoolimata oleks andmekaitsenõukogu pooldanud seda, et andmekaitseraamistiku üle peetud läbirääkimistel oleks käsitletud rohkem küsimusi, mis tuvastati i) artikli 29 töörühma arvamuses 01/2016 ja ii) varasemates ühistes läbivaatamistes[30].

35. Samuti märgib andmekaitsenõukogu, et hoolimata mitmest muudatusest ja täiendavast selgitusest otsuse eelnõu põhjendustes ei ole andmekaitseraamistiku põhimõtted, mida raamistikuga hõlmatud organisatsioonid peavad järgima, andmekaitseraamistiku Privacy Shield alusel kohaldatavate põhimõtetega võrreldes sisuliselt muutunud.

1.3.7 Ebaselgus andmekaitseraamistiku dokumentides

36. Andmekaitsenõukogu märgib, et lisade ülesehituse ja nende nummerduse tõttu on suhteliselt keeruline teavet leida ja sellele tugineda. See suurendab veelgi uue raamistiku üldist keerukat esitlust –raamistiku lisadesse on koondatud erineva õigusliku kaaluga dokumendid – ja selle tulemusel ei

[27] Otsuse eelnõu I lisa II jao punkt 2.

[28] Lisamärkusi ELi-USA andmekaitseraamistikuga hõlmatud isikuandmete kasutamise kohta õiguskaitse eesmärkidel on esitatud käesoleva arvamuse punktis 3.1.

[29] Lisamärkusi ELi-USA andmekaitseraamistikuga hõlmatud isikuandmete kasutamise kohta riikliku julgeoleku eesmärkidel on esitatud käesoleva arvamise punktis 3.2.

[30] Iga-aastased läbivaatamised: ELi-USA andmekaitseraamistik – esimene iga-aastane läbivaatamine, WP 255, artikli 29 töörühma aruanne (vastu võetud 28. novembril 2017) (edaspidi „esimese ühise läbivaatamise aruanne“); ELi-USA andmekaitseraamistik – teine iga-aastane läbivaatamine, andmekaitsenõukogu aruanne (vastu võetud 22. jaanuaril 2019) (edaspidi „teise ühise läbivaatamise aruanne“); ELi-USA andmekaitseraamistik – kolmas iga-aastane läbivaatamine, andmekaitsenõukogu aruanne (vastu võetud 12. novembril 2019) (edaspidi „kolmanda ühise läbivaatamise aruanne“).

pruugi andmesubjektid, andmekaitseraamistikuga hõlmatud organisatsioonid ja ELi andmekaitseasutused andmekaitseraamistiku põhimõtetest hästi aru saada.

37. Ühtlasi rõhutab andmekaitsenõukogu, et andmekaitseraamistikus tuleks kasutada terminoloogiat järjepidevalt. Praegu ei tehta seda näiteks mõiste „töötlemine“ puhul. Andmekaitseraamistiku mõnes osas on tõepoolest loetletud teatavad andmetöötlustoimingute liigid, selle asemel et kasutada terminit „töötlemine“. See võib tekitada õiguskindlusetust ja võimalikke lünki kaitses[31].

38. Andmekaitsenõukogu tunneb heameelt selle üle, et andmekaitseraamistikus on esitatud mõne kasutatud termini määratlused[32]. Seda ei ole aga tehtud teatavate muude oluliste terminite puhul, näiteks „esindaja“ või „volitatud töötleja“, mille kohta tuleks andmekaitsenõukogu arvamuse kohaselt esitada andmekaitseraamistiku I lisa I jao punktis 8 selge ja konkreetne määratlus, millega nii USA kui ka EL nõustuvad, et vältida segadust andmekaitseraamistikule tuginevate andmekaitseraamistikuga hõlmatud organisatsioonide, järelevalveasutuste ja üldsuse hulgas hilisemas etapis.

39. Mis puudutab mõiste „personaliandmed“ lahknevaid tõlgendusi ELis ja USAs, siis nõustub andmekaitsenõukogu komisjoni kolmanda läbivaatamise aruandes esitatud eesmärgiga jätkata arutelusid USA ametiasutustega[33].

2 ANDMEKAITSE ÜLDISED ASPEKTID

2.1 Üldpõhimõtted

2.1.1 Mõisted

40. Isikuandmete kaitse üldmäärust käsitleva kaitse piisavuse viitedokumendi põhjal peaks kolmanda riigi õigusraamistik sisaldama peamisi andmekaitsemõisteid ja/või -põhimõtteid. Need ei pea küll täpselt vastama isikuandmete kaitse üldmääruses kasutatud terminoloogiale, kuid peaksid kajastama Euroopa andmekaitseõiguses sätestatud mõisteid ja olema nendega kooskõlas. Isikuandmete kaitse üldmäärus sisaldab näiteks järgmisi olulisi mõisteid: „isikuandmed“, „isikuandmete töötlemine“, „vastutav töötleja“, „volitatud töötleja“, „vastuvõtja“ ja „tundlikud andmed“. Andmekaitsenõukogu tunneb heameelt selle üle, et sarnaselt andmekaitseraamistikule Privacy Shield sisaldab andmekaitseraamistik terminite „isikuandmed“, „töötlemine“ ja „vastutav töötleja“ määratlusi.

41. Andmekaitsenõukogu märgib, et ebaselgeks jääb see, kui suures ulatuses kohaldatakse andmekaitseraamistiku põhimõtteid andmekaitseraamistikuga hõlmatud organisatsioonide suhtes, kes saavad ELilt isikuandmeid üksnes töötlemise eesmärgil („esindajad“ või „volitatud töötlejad“). Andmekaitseraamistikus ei eristata esindajate ja vastutavate töötlejate suhtes kohaldatavaid

[31] Näiteks i) otsuse eelnõu I lisa III jao punkti 6 alapunkti f sõnastuse kohaselt on andmekaitseraamistiku põhimõtted kohaldatavad ainult siis, kui organisatsioon saadud andmeid säilitab, kasutab või avalikustab (see tähendab mitte muude terminiga „töötlemine“ hõlmatud toimingute, näiteks kogumise, salvestamise, muutmise, väljavõtete tegemise, järelpärimise tegemise või kustutamise puhul), ja ii) otsuse eelnõu I lisa II jao punkti 4 alapunkti a kohaselt kehtib andmete turvalisuse nõue üksnes isikuandmete tekitamise, säilitamise, kasutamise või levitamise puhul.

[32] Otsuse eelnõu I lisa I jao punkt 8.

[33] Kolmanda ühise läbivaatamise aruanne, lk 5, 15–16 ja 30. Vt ka komisjoni talituste töödokument, mis on lisatud komisjoni aruandele Euroopa Parlamendile ja nõukogule ELi-USA andmekaitseraamistiku Privacy Shield toimimise kolmanda iga-aastase läbivaatamise kohta, lk 17–18.

andmekaitseraamistiku põhimõtteid, kuigi mitu raamistiku põhimõtetes sisalduvat kohustust ei ole esindajate / volitatud töötlejate puhul sobilikud. Näiteks ei peaks esindajal / vastutaval töötlejal olema võimalik esitada üksikisikutele täieliku teate kõiki elemente, nagu on nõutud teate põhimõttega (näiteks eesmärke, milleks ta isikuandmeid kogub ja kasutab)[34], sest esindaja / volitatud töötleja ei saa töötlemise vahendeid ja eesmärke üksinda kindlaks määrata[35].

2.1.2 Eesmärgi piiramise põhimõte

42. Kooskõlas isikuandmete kaitse üldmäärusega on isikuandmete kaitse üldmäärust käsitlevas kaitse piisavuse viitedokumendis sätestatud, et isikuandmeid tuleks töödelda konkreetsel eesmärgil ja kasutada seejärel üksnes määral, mil see vastab töötlemise eesmärgile.

43. Andmete terviklikkuse ja eesmärgi piiramise põhimõtte kohaselt ei tohi organisatsioon töödelda isikuandmeid viisil, mis ei vasta eesmärkidele, milleks need koguti või milleks üksikisik järgnevalt loa andis[36]. Andmekaitsenõukogu märgib, et teate, valikuvõimaluse ning andmete terviklikkuse ja eesmärgi piiramise põhimõtetes on kasutatud erinevat terminoloogiat. Nagu artikli 29 töörühm märkis ja hoolimata kasulikest selgitustest otsuse eelnõu põhjendustes, kasutatakse andmekaitseraamistikus selliseid termineid nagu „erinevad eesmärgid“, „oluliselt erinevad“ eesmärgid või „kasutamine, mis ei ole kooskõlas“ ilma neid mõisteid raamistikus selgelt määratlemata, mis võib tekitada õiguskindlusetust.

2.1.3 Õigus andmetega tutvuda, nõuda andmete parandamist ja kustutamist ning esitada vastuväiteid

44. Andmekaitseraamistikus on andmesubjektide õigust andmetega tutvuda ning nõuda nende parandamist ja kustutamist käsitletud juurdepääsu põhimõttes[37].

45. Andmekaitseraamistikuga Privacy Shield võrreldes ei ole juurdepääsu põhimõtet muudetud. Sellest tulenevalt esinevad jätkuvalt teatavad probleemid, mida väljendati artikli 29 töörühma arvamuses 01/2016 ja mida on üksikasjalikult kirjeldatud allpool.

46. Mis puudutab üksikisikute õigust andmetega tutvuda, siis peab andmekaitsenõukogu vajalikuks korrata, et üksikisikute päringutele vastamise kohustust käsitlevad üksikasjad oleks parem esitada põhimõtte põhitekstis (neid on endiselt kirjeldatud ainult joonealuses märkuses[38]).). Samuti peaks olema selge, et juurdepääs tuleb anda sel määral, mil andmekaitseraamistikuga hõlmatud organisatsioon isikuandmeid töötleb, mitte ainult siis, kui ta neid säilitab[39]. Andmekaitsenõukogu arvamuse kohaselt tekitab praegune sõnastus olukorra, kus õigust andmetega tutvuda tõlgendatakse liiga kitsalt.

[34] Otsuse eelnõu I lisa II jao punkti 1 alapunkt a.
[35] Vt ka artikli 29 töörühma arvamus 01/2016, lk 16.
[36] Otsuse eelnõu I lisa II jao punkt 5.
[37] Otsuse eelnõu I lisa II jao punkt 6 ja III jao punkti 8 alapunkti a alapunkt i.
[38] Otsuse eelnõu I lisa III jao punkti 8 alapunkti a alapunkti i alapunkt 1 – joonealune märkus nr 14.
[39] Otsuse eelnõu I lisa III jao punkti 8 alapunkti d alapunkt ii.

47. Seoses juurdepääsuõigusest tehtavate erandite loeteluga[40] kaitstakse mõne erandiga jätkuvalt pigem andmekaitseraamistikuga hõlmatud organisatsioonide huve. Andmekaitsenõukogu tunneb jätkuvalt muret selle üle, et nendel juhtudel ei tundu kehtivat nõue võtta arvesse üksikisiku õigusi ja huvisid[41].

48. Veel üks erand, mille üle artikli 29 töörühm on varem muret väljendanud[42] ja mis tundub andmekaitsenõukogule liiga lai, on erand juurdepääsuõigusest avalikult kättesaadavale teabele ja avalikest registritest saadud teabele[43]. Andmekaitsenõukogu on korduvalt märkinud, et ELi õiguse kohaselt on andmesubjektidel alati õigus oma andmetega tutvuda, olenemata sellest, kas need isikuandmed on avaldatud. Kui taotlus andmetega tutvuda lükatakse tagasi põhjusel, et andmed on saadud avalikult kättesaadavatest allikatest või avalikest registritest, kaotab isik võimaluse kontrollida andmete täpsust ja veenduda selles, kas andmete avalikustamine oli üldse seaduslik.

49. Andmekaitsenõukogu tuletab meelde, et õigus andmetega tutvuda on sätestatud harta artikli 8 lõikes 2. Ehkki tegemist ei ole absoluutse õigusega, on see seoses õigusega isikuandmete kaitsele väga oluline, sest see muudab andmesubjekti jaoks lihtsamaks teiste õiguste, näiteks andmete parandamise ja kustutamise ning vastuväite esitamise õiguse kasutamise[44].

50. Lisaks õigusele andmetega tutvuda ja nõuda nende kustutamist peaks andmesubjektidel olema õigus esitada oma konkreetse olukorraga seotud õigustatud ja veenvatel põhjustel kolmanda riigi õigusraamistikus kehtestatud eritingimustel igal ajal vastuväide oma andmete töötlemisele[45].

51. Valikuvõimaluse põhimõtte kaudu nähakse andmekaitseraamistikuga ette õigus keelduda isikuandmete edastamisest kolmandale isikule või isikuandmete kasutamisest algsest eesmärgist oluliselt erineval eesmärgil[46]. Peale selle on üksikisikutel alati õigus keelduda oma isikuandmete kasutamisest otseturunduse eesmärgil[47]. Selle õiguse kasutamise viisi, eeskätt selle aega, ei ole üksikasjalikult kirjeldatud, välja arvatud otseturunduse eesmärkide puhul. Seepärast kutsub andmekaitsenõukogu komisjoni selgitama, kuidas üksikisikud saavad vastuväite esitamise õigust kasutada.

52. Nagu on märgitud artikli 29 töörühma arvamuses 01/2016, leiab andmekaitsenõukogu, et lihtne viide selle õiguse olemasolule ei ole piisav. Pakkuda tuleks individuaalset võimalust seda õigust kasutada ja mitte üksnes isikuandmete avalikustamise või uuesti kasutamise korral. Andmekaitsenõukogu rõhutab, et andmekaitseraamistikuga tuleks tagada üldine õigus esitada vastuväide andmesubjekti konkreetse olukorraga seotud õigustatud ja veenvatel põhjustel. Andmekaitsenõukogu soovitab tagada sellise vastuväite esitamise õiguse igal ajal ja mitte piirata seda õigust andmete kasutamisega otseturunduse eesmärgil[48].

53. Mis puudutab personaliandmeid, siis hindab andmekaitsenõukogu komisjoni selgitusi teate ja valikuvõimaluse põhimõtete kohaldamise kohta olukorras, kus põhimõtete järgimist kinnitanud USA organisatsioon kavatseb kasutada personaliandmeid muul kui töösuhtega seotud eesmärgil, näiteks

[40] Otsuse eelnõu I lisa III jao punkti 8 alapunkt e.
[41] Artikli 29 töörühma arvamus 01/2016, punkt 2.2.5.
[42] Artikli 29 töörühma arvamus 01/2016, punkt 2.2.9.
[43] Otsuse eelnõu I lisa III jao punkti 15 alapunktid d–e.
[44] Artikli 29 töörühma arvamus 01/2016, punkt 2.2.5.
[45] Isikuandmete kaitse üldmäärust käsitlev kaitse piisavuse viitedokument, punkt 3.A.8.
[46] Otsuse eelnõu I lisa II jao punkti 2 alapunkt a.
[47] Otsuse eelnõu I lisa III jao punkti 12 alapunkt a.
[48] Artikli 29 töörühma arvamus 01/2016, punkt 2.2.2.

reklaamteadeteks[49]. Andmekaitsenõukogu jääb aga oma seisukoha juurde, et personaliandmete edasist töötlemist muul kui töösuhtega seotud eesmärgil käsitatakse enamikul juhtudel algsele eesmärgile mittevastavana ning töösuhte kontekstis on nõusoleku andmine harva täiesti vabatahtlik.

54. Samuti kordab andmekaitsenõukogu artikli 29 töörühma väljendatud muret seoses teate ja valikuvõimaluse põhimõtetest personaliandmete puhul tehtava erandiga „[s]elles ulatuses ja ajavahemikuks, mis on vajalik organisatsiooni teovõime kahjustamise vältimiseks edutamiste, ametisse nimetamiste või muude sarnaste töösuhet puudutavate otsuste langetamiseks“,[50] mis tundub andmekaitsenõukogule olevat liiga lai ja ebamäärane[51].

2.1.4 Andmete edasisaatmise piirangud

55. Isikuandmete esmasel vastuvõtjal tuleks lubada saadud andmeid edasi saata vaid juhul, kui andmete järgmise vastuvõtja suhtes (see tähendab isiku suhtes, kellele andmed edasi saadetakse) kohaldatakse samuti eeskirju (sealhulgas lepingust tulenevaid nõudeid), mis tagavad piisava kaitsetaseme, ja kui kõnealune isik järgib vastutava töötleja nimel andmete töötlemisel asjakohaseid juhiseid. Andmete edasisaatmine ei tohi kahjustada nendele üksikisikutele tagatud kaitse taset, kelle andmeid edastatakse. EList edastatud andmete esmane vastuvõtja peab tagama, et kaitse piisavuse otsuse puudumisel on seoses andmete edasisaatmisega ette nähtud piisavad kaitsemeetmed. Selline andmete edasisaatmine peaks toimuma vaid piiratud ja kindlaksmääratud eesmärkidel ning üksnes seni, kuni selliseks töötlemiseks on õiguslik alus[52].

56. Andmekaitseraamistiku kohase andmete kolmandale isikule edastamise eest vastutuse põhimõtte alusel võib andmeid edasi saata ainult piiratud ja konkreetsel eesmärgil andmekaitseraamistikuga hõlmatud organisatsiooni ja kolmanda isiku vahelise lepingu (või sellega võrreldava kontsernisisese kokkuleppe) alusel ning üksnes juhul, kui nimetatud lepinguga nõutakse kolmandalt isikult samal tasemel kaitse pakkumist, nagu on tagatud andmekaitseraamistiku põhimõtetega[53].

57. Andmekaitsenõukogu soovib korrata artikli 29 töörühma arvamuses 01/2016 väljendatud muret seoses vastutavate töötlejate vahelise kontsernisisese andmeedastuse puhul kehtiva erandiga lepingu sõlmimise vajadusest[54]. Seoses personaliandmetega ei mõista andmekaitsenõukogu jätkuvalt, millel põhineb erand kohustusest sõlmida kolmandast isikust vastutava töötlejaga leping juhul, kui andmeid saadetakse edasi „juhuslikeks töösuhtega seotud operatiivvajadusteks“[55].

58. Peale selle soovib andmekaitsenõukogu korrata artikli 29 töörühma esitatud nõuet,[56] mille kohaselt organisatsioonid, kelle jaoks raamistik on siduv, peaksid enne andmete edasisaatmist hindama, kas andmete saaja suhtes kohaldatavad kolmanda riigi õigusaktide kohased kohustuslikud nõuded ei kahjusta nende andmesubjektide kaitse jätkumist, kelle andmeid edastatakse[57].

---

[49] Otsuse eelnõu I lisa III jao punkti 9 alapunkti b alapunkt i ning põhjendus 15 ja joonealune märkus nr 27.
[50] Otsuse eelnõu I lisa III jao punkti 9 alapunkti b alapunkt iv.
[51] Artikli 29 töörühma arvamus 01/2016, punkt 2.2.7.
[52] Isikuandmete kaitse üldmäärust käsitlev kaitse piisavuse viitedokument, punkt 3.A.9.
[53] Otsuse eelnõu I lisa II jao punkt 3.
[54] Otsuse eelnõu I lisa III jao punkti 10 alapunkti b alapunkti, kus on viidatud „või muudele grupisisestele vahenditele (nt vastavuse ja kontrolli programmid)“, mis ilmselt ei pea olema siduvad.
[55] Otsuse eelnõu I lisa III jao punkti 9 alapunkti e alapunkti, kus on viidatud sellistele näidetele nagu kindlustuskate.
[56] Artikli 29 töörühma arvamus 01/2016, punkt 2.2.3, lk 21.
[57] Kohtuotsust Schrems II arvesse võttes on andmekaitsenõukogu täiendavalt selgitanud andmeeksportijate ja -importijate kohustusi seoses andmete edasisaatmisega mitmes suunises ja soovituses; vt andmekaitsenõukogu

59. Andmekaitsenõukogu jääb oma seisukoha juurde, et isikuandmete edasisaatmisega kolmandatele riikidele võib kaasneda üksikisikute põhiõigustesse sekkumine, ning kutsub komisjoni selgitama, et kaitsemeetmed, mille andmete algne saaja kolmandas riigis asuvale andmeimportijale kehtestab, peavad enne andmete andmekaitseraamistikus edasisaatmist olema tõhusad, võttes arvesse kolmanda riigi õigusakte[58].

2.1.5 Automatiseeritud otsuste tegemine ja profiilianalüüs

60. Otsuseid, mis põhinevad üksnes isikuandmete automatiseeritud töötlemisel (automatiseeritud üksikotsuste tegemine), sealhulgas profiilianalüüsil, ja mis toovad kaasa õiguslikke tagajärgi või avaldavad andmesubjektile olulist mõju, võib teha üksnes teatavatel kolmanda riigi õigusraamistikus kehtestatud tingimustel. Euroopa õigusraamistikus kuuluvad selliste tingimuste hulka näiteks vajadus saada andmesubjektilt sõnaselge nõusolek või sellise otsuse vajalikkus lepingu sõlmimiseks. Andmesubjektil peaks olema õigus sellele, et tema kohta ei tehta otsust, mis ei ole kooskõlas selliste kolmanda riigi õigusraamistikus sätestatud tingimustega. Kolmanda riigi õiguses peaksid igal juhul olema ette nähtud vajalikud kaitsemeetmed, sealhulgas õigus saada teavet otsuse tegemise konkreetsete põhjuste ja kasutatud loogika kohta, õigus ebaõige või mittetäieliku teabe parandamisele ning õigus otsus vaidlustada, kui selle vastuvõtmisel on lähtutud ebaõigetest faktidest[59].

61. Andmekaitseraamistikuga ei ole ette nähtud mingeid õiguslikke tagatisi juhuks, kui üksikisikute kohta tehakse õiguslike tagajärgedega või märkimisväärse mõjuga otsuseid üksnes selliste andmete automatiseeritud töötlemise põhjal, mille eesmärk on anda hinnang nende teatavatele isikuomadustele, näiteks tööviljakusele, krediidivõimelisusele, usaldusväärsusele või käitumisele.

62. Nagu on juba märgitud artikli 29 töörühma arvamuses 01/2016 ja andmekaitsenõukogu varasemates arvamustes kaitse piisavuse kohta Jaapanis ja Lõuna-Koreas,[60] leiab andmekaitsenõukogu, et kiire arengu tõttu automatiseeritud otsuste tegemise ja profiilianalüüsi – mis üha enam toimub tehisintellektipõhise tehnoloogia abil – valdkonnas tuleb sellele erilist tähelepanu pöörata[61].

63. Andmekaitsenõukogu võtab teadmiseks komisjoni argumendid, mille kohaselt automatiseeritud otsuste tegemist käsitlevate erinormide puudumine andmekaitseraamistikus tõenäoliselt ei mõjuta liidus kogutud isikuandmete kaitse taset (sest tavaliselt teeb kõik automatiseeritud otsused liidus asuv vastutav töötleja, kellel on asjaomase andmesubjektiga otsene suhe)[62].. Andmekaitsenõukogu arvamuse kohaselt ei saa aga välistada, et USAs asuv vastutav töötleja teeb otsuse eelnõu alusel

---

soovitused 01/2020 edastusvahendeid täiendavate meetmete kohta, et tagada vastavus isikuandmete kaitse ELi tasemega (versioon 2.0, vastu võetud 18. juunil 2021); soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis (vastu võetud 10. novembril 2020); suunised 04/2021 toimimisjuhendite kui andmeedastusvahendite kohta (versioon 2.0, vastu võetud 22. veebruaril 2022); soovitused 1/2022 heakskiitmistaotluse ning vastutavale töötlejale siduvates kontsernisisestes eeskirjades sisalduvate elementide ja põhimõtete kohta (vastu võetud 14. novembril 2022); suunised 07/2022 sertifitseerimise kui edastamisvahendi kohta (vastu võetud pärast avalikku konsultatsiooni 14. veebruaril 2023).

[58] Artikli 29 töörühma arvamus 01/2016, punkt 2.2.3, lk 21.

[59] Isikuandmete kaitse üldmäärust käsitlev kaitse piisavuse viitedokument, punkt 3.B.3.

[60] Andmekaitsenõukogu arvamus 28/2018 Euroopa Komisjoni rakendusotsuse eelnõu kohta, mis käsitleb isikuandmete kaitse piisavust Jaapanis (vastu võetud 5. detsembril 2018); andmekaitsenõukogu arvamus 32/2021 Euroopa Komisjoni rakendusotsuse eelnõu kohta, mis käsitleb isikuandmete kaitse piisavust Korea Vabariigis (vastu võetud 24. septembril 2021).

[61] Vt muu hulgas kohtuasi C-634/21, OQ *vs.* Land Hesse (SCHUFA Holding ja teised), eelotsusetaotlus (menetlemine pooleli).

[62] Otsuse eelnõu põhjendused 33 ja 34.

edastatud andmete puhul otsuseid automatiseeritud töötluse põhjal (näiteks seoses töösuhtega, töötulemuste hindamise, kindlustuse ja eluasemega).

64. Andmekaitsenõukogu tunneb heameelt komisjoni viidete üle konkreetsetele kaitsemeetmetele, mis on USA asjaomaste õigusaktidega eri valdkondades ette nähtud[63]. Andmekaitsenõukogule tundub aga, et üksikisikutele tagatud kaitse tase on erinev, sõltuvalt sellest, milliseid sektoripõhiseid eeskirju (kui üldse) konkreetse olukorra suhtes kohaldatakse. Esineb oht, et teatavaid olukordi ei ole käsitletud, sest need ei jää osutatud õigusaktide kohaldamisalasse. Peale selle on automatiseeritud otsuste tegemisega seotud üksikute õiguste sisu kirjeldatud eri õigusaktides erinevalt.

65. Sellel taustal leiab andmekaitsenõukogu, et andmekaitseraamistikus on vaja erieeskirju automatiseeritud otsuste tegemise kohta, et tagada piisavad kaitsemeetmed, sealhulgas üksikisiku õigus teada kasutatavat loogikat, õigus otsus vaidlustada ja õigus otsesele isiklikule kontaktile, kui otsus teda oluliselt mõjutab[64].

2.2 Menetluslikud ja nõuete täitmise tagamise mehhanismid

66. Andmekaitsenõukogu märgib, et andmekaitseraamistikus tuginetakse jätkuvalt organisatsioonide enda esitatava kinnituse süsteemile, kuigi komisjon nimetab seda sertifitseerimissüsteemiks.

67. Andmekaitsenõukogu tuletab meelde varasemate ühiste läbivaatamiste käigus tehtud täiustusi. Need on seotud näiteks kaubandusministeeriumi rolliga organisatsioonide enda kinnituse (uuesti) esitamise protsessis, äriühingute andmekaitseraamistiku põhimõtetest kinnipidamise jälgimise (näiteks kohapealsete kontrollide ja nõuetele vastavust käsitlevate küsimustike kasutamise teel) ning osalemise kohta esitatud valeandmete kindlakstegemise ja nendega tegelemisega.

68. Samal ajal on artikli 29 töörühm ja andmekaitsenõukogu väljendanud muret seoses andmekaitseraamistiku Privacy Shield nõuete täitmise üle tehtava järelevalve teatava puudulikkusega[65]. Eelkõige nõustub andmekaitsenõukogu järeldustega, mille komisjon tegi pärast andmekaitseraamistiku Privacy Shield kolmandat iga-aastast läbivaatamist ning mille kohaselt kaubandusministeeriumi kohapealsed kontrollid andmekaitseraamistiku Privacy Shield alusel piirdusid üldjuhul vorminõuetega (näiteks määratud kontaktpunktide ebapiisav reageerimine või asjaolu, et äriühingu tegevuspõhimõtted eraelu puutumatuse kohta ei ole veebis kättesaadavad)[66]. Andmekaitsenõukogu leiab, et sisulisemate nõuete täitmise üle tehtavad kontrollid on äärmiselt olulised.

69. Samuti tuletab andmekaitsenõukogu meelde tõhusa järelevalve (sealhulgas sisuliste nõuete täitmise üle tehtava järelevalve) ja andmekaitseraamistiku järgimise tagamise tähtsust. Andmekaitsenõukogu jälgib seda aspekti hoolikalt, muu hulgas korrapäraste läbivaatamiste raames.

70. Seoses nõuete täitmise tagamisega võtab andmekaitsenõukogu teadmiseks FTC[67] ja transpordiministeeriumi[68] kirjades uuesti võetud kohustused käsitada prioriteetsena andmekaitseraamistiku väidetavate rikkumiste uurimist, võtta asjakohaseid nõuete täitmise tagamise

[63] Otsuse eelnõu põhjendus 35.
[64] Vt ka kolmanda ühise läbivaatamise aruande punkt 76.
[65] Kolmanda ühise läbivaatamise aruande punkt 7.
[66] Komisjoni aruanne Euroopa Parlamendile ja nõukogule ELi-USA andmekaitseraamistiku Privacy Shield toimimise kolmanda iga-aastase läbivaatamise kohta (23. oktoober 2019, COM(2019) 495 final), lk 4.
[67] Otsuse eelnõu IV lisa.
[68] Otsuse eelnõu V lisa.

meetmeid üksuste suhtes, kes on esitanud raamistikus osalemise kohta valesid või pettusel põhinevaid andmeid, jälgida andmekaitseraamistiku rikkumist käsitlevaid täitekorraldusi ja teha koostööd ELi andmekaitseasutustega. Sellega seoses tunnustab andmekaitsenõukogu ka FTC viidet sellele, et eelduste kohaselt keskendub ta oma nõuete täitmise tagamise alases tegevuses veelgi rohkem andmekaitseraamistiku rikkumistele ja kavatseb viia läbi uurimisi (muu hulgas) omal algatusel. Andmekaitsenõukogu jälgib neid aspekte hoolikalt, muu hulgas korrapäraste läbivaatamiste raames.

2.3 Õiguskaitsemehhanismid

71. Andmekaitsenõukogu tunneb heameelt selle üle, et otsuse eelnõus on selgelt esitatud ELi andmesubjektide jaoks seitse õiguskaitsevahendit, kui nende isikuandmete töötlemisel rikutakse andmekaitseraamistikku[69].

72. Need erinevad kaebuste käsitlemise mehhanismid on kehtestatud kooskõlas kaebuste käsitlemise, nõuete täitmise tagamise ja vastutuse põhimõtte ning kaubandusministeeriumi välja antud täiendava põhimõtte nr 11 „Vaidluste lahendamine ja täitmise tagamine“ nõuetega, mida on nimetatud otsuse eelnõu I lisas[70].

73. Nagu komisjon oma otsuse eelnõus rõhutas, „tuleks andmesubjektile ette näha tõhus haldus- ja õiguskaitse“[71]. See kajastab isikuandmete kaitse üldmääruse artikli 45 lõike 2 punktis a sätestatud nõuet, mille kohaselt peab komisjon oma hinnangus kolmandas riigis tagatud kaitse taseme piisavuse kohta võtma eelkõige arvesse „tõhusa haldus- ja õiguskaitse olemasolu andmesubjektide jaoks, kelle isikuandmeid edastatakse“[72]. Seda nõuet tuletatakse meelde ka isikuandmete kaitse üldmäärust käsitlevas kaitse piisavuse viitedokumendis[73].

74. Andmekaitsenõukogu märgib, et need õiguskaitsemehhanismid on samad kui endises andmekaitseraamistikus Privacy Shield sisalduvad mehhanismid, mille kohta artikli 29 töörühm on märkusi esitanud[74].

75. Seoses vahekohtumehhanismiga märgib andmekaitsenõukogu, et andmekaitseraamistiku põhimõtete erandite puhul ei saa seda võimalust kasutada[75], ja osutab seega oma märkustele, mis on esitatud punktis 33.

76. Mis puudutab täiendavaid õiguskaitsevõimalusi USA õiguse alusel, siis tunneb andmekaitsenõukogu heameelt ka täpsemate üksikasjade üle nimetatud õigusaktides[76] ja osutab oma märkustele, mis on esitatud punktis 21.

77. Lisaks tunneb andmekaitsenõukogu heameelt FTC kirja üle, milles on kirjeldatud föderaalse kaubanduskomisjoni kavatsust teha tihedat koostööd ELi andmekaitseasutustega[77]. Samuti tunneb

[69] Otsuse eelnõu põhjendus 67.
[70] Otsuse eelnõu I lisa II jao punkt 7 ja III jao punkt 11 ning I lisa I lisa.
[71] Otsuse eelnõu põhjendus 64.
[72] Vt ka isikuandmete kaitse üldmääruse põhjendus 141, kus on viidatud Euroopa Liidu põhiõiguste harta artiklile 47, mis käsitleb õigust tõhusale õiguskaitsevahendile ELis.
[73] Isikuandmete kaitse üldmäärust käsitlev kaitse piisavuse viitedokument, lk 8.
[74] Vt eelkõige artikli 29 töörühma arvamus 01/2016, punkti 2.2.6 alapunkta.
[75] Otsuse eelnõu I lisa I lisa A jagu.
[76] Otsuse eelnõu põhjendus 85.
[77] Otsuse eelnõu IV lisa.

andmekaitsenõukogu heameelt selle üle, et FTC prioriseerib kaebuste lahendamist, kuigi see ei pruugi anda andmesubjektidele kindlust selle kohta, et nende kaebusi kõikidel juhtudel käsitletakse.

78. Seoses asjaoluga, et teatavatel juhtudel on üksikisikutel võimalik esitada kaebus ELi andmekaitseasutusele, sooviks andmekaitsenõukogu saada rohkem teavet selle kohta, i) kas ELi andmekaitseasutuste võimalus anda nõu kaitse- või hüvitamismeetmete kohta võiks hõlmata trahvide või uurimisvolituste kasutamise soovitamist ning ii) mil määral FTC või transpordiministeerium ELi andmekaitseasutuste meetmeid nõuete täitmise tagamise meetmetes tõendina arvesse võtaks[78].

79. Andmekaitsenõukogu jälgib hoolikalt nende õiguskaitsemehhanismide tõhusust, muu hulgas korrapäraste läbivaatamiste raames.

3 JUURDEPÄÄS EUROOPA LIIDUST EDASTATUD ISIKUANDMETELE JA NENDE KASUTAMINE USAs ASUVATE AVALIKU SEKTORI ASUTUSTE POOLT

3.1 Andmetele juurdepääs ja nende kasutamine kriminaalõiguskaitse eesmärkidel

3.1.1 Õiguskaitseasutuste juurdepääs isikuandmetele peaks põhinema selgetel, täpsetel ja ligipääsetavatel eeskirjadel

80. Andmekaitsenõukogu tunneb heameelt otsuse eelnõus varasema kaitse piisavuse otsusega võrreldes üksikasjalikumalt esitatud teabe ja täpsemate selgituste üle seoses USA avaliku sektori asutuste poolt kriminaalõiguskaitse eesmärkidel isikuandmetele juurdepääsu ja nende andmete kasutamisega. Otsuse eelnõu VI lisas on esitatud ka USA justiitsministeeriumi kriminaalõiguskaitseosakonna kiri, milles „antakse lühike ülevaade peamisetest uurimisvahenditest, mida kasutatakse Ameerika Ühendriikide äriühingutelt kaubandusandmete ja muude registriandmete saamiseks kriminaalõiguskaitse või avaliku huviga seotud (tsiviil- ja õiguslikel) eesmärkidel, sealhulgas nende asutuste kehtestatud juurdepääsupiirangute kohta“. Kirja kohaselt kasutatakse kõiki selles kirjeldatud õiguslikke menetlusi USAs asuvatelt äriühingutelt teabe saamiseks, sõltumata andmesubjekti kodakondsusest või elukohast, ning need põhinevad otseselt USA põhiseadusel (neljas muudatus), asjaomastel seadustel ja menetlusõigusel või justiitsministeeriumi suunistel ja meetmetel. Selles ülevaates ei käsitleta riikliku julgeolekuga seotud uurimisvahendeid, mida õiguskaitseasutused kasutavad terrorismi- ja muude riikliku julgeoleku alastes uurimistes[79].

81. Andmekaitsenõukogu märgib, et otsuse eelnõus ja selle VI lisas on arutatud peamiselt föderaalse õiguse täitmise tagamist ja reguleerivaid asutusi[80] ning seal ei ole konkreetselt viidatud osariikide seadustele, millega need teabe hankimise menetlused on ette nähtud. Samuti on VI lisas mainitud, et „[ä]riühingutel on muid õiguslikke aluseid, et vaidlustada haldusasutuste andmetaotlusi, mis põhinevad nende konkreetsel sektoril ja olemasolevate andmete liigil“, ning lisaks esitatud mitut näidet hõlmav mittetäielik loetelu, nagu pangasaladuse seadus (Bank Secrecy Act) ja selle rakendusmäärused,[81] õiglase krediidiinfo seadus (Fair Credit Reporting Act)[82] ja finantsandmetega

[78] Otsuse eelnõu I lisa III jao punkti 5 alapunkti b alapunkt iii.
[79] Otsuse eelnõu VI lisa joonealune märkus nr 1.
[80] Vt otsuse eelnõu põhjendused 90–93.
[81] 31 U.S.C. § 5318; 31 C.F.R. X peatükk.
[82] 15 U.S.C. § 1681b.

seotud eraelu puutumatuse seadus (Right to Financial Privacy Act)[83]. Andmekaitsenõukogu märgib, et konkreetse juurdepääsutaotluse õiguslik alus sõltub taotletavate andmete laadist, äriühingu õiguslikust vormist, õigusliku menetluse laadist (õigus- või haldusmenetlus, muu avaliku huviga seotud menetlus) ning juurdepääsu taotleva üksuse liigist. Kuna kõik kohaldatavad eeskirjad, millega õiguskaitseasutuste juurdepääsu USAsse edastatud andmetele piiratakse, põhinevad põhiseadusel, asjaomastel seadustel ja justiitsministeeriumi läbipaistvatel tegevuspõhimõtetel, siis tunnistab andmekaitsenõukogu nende eeskirjade kättesaadavust ja kutsub komisjoni seda aspekti otsuse eelnõus kajastama. VI lisast tuleneb, et neid seadusi kohaldatakse sõltumata andmesubjekti kodakondsusest või elukohast ning üldjuhul hõlmavad need põhiseaduse neljanda muudatuse kohaseid nõudeid (kuigi sageli lähevad need neist nõuetest kaugemale ja sisaldavad täiendavat kaitset).

82. Kokkuvõttes märgib andmekaitsenõukogu, et võrreldes eelmise kaitse piisavuse otsusega sisaldab otsuse eelnõu üksikasjalikumat hinnangut föderaalsete õiguskaitseasutuste juurdepääsu kohta. Mis puudutab osariikide õiguskaitseasutuste juurdepääsu, siis märgib andmekaitsenõukogu samuti, et VI lisa kohaselt peab osariigi õigusega tagatud kaitse olema vähemalt samaväärne USA põhiseadusega, sealhulgas selle neljanda muudatusega tagatud kaitsele. Andmekaitsenõukogu kutsub komisjoni tulevastes läbivaatamistes täiendavalt hindama osariikide õigusega pakutava kaitse elementi.

3.1.2 Taotletavate seaduslike eesmärkide vajalikkust ja proportsionaalsust on vaja tõendada

83. Andmekaitsenõukogu märgib, et andmetele juurdepääsu taotlemist õiguskaitse eesmärgil võidakse üldiselt käsitleda seadusliku eesmärgi järgimisena. Samal ajal on sellised riived vastuvõetavad üksnes juhul, kui need on vajalikud ja proportsionaalsed[84].

84. Vastavalt Euroopa Liidu Kohtu väljakujunenud praktikale nõutakse proportsionaalsuse põhimõtte alusel, et seadusandlikud meetmed, millega nähakse ette sekkumine õigusesse eraelule ja isikuandmete kaitsmisele, oleksid „vastava õigusaktiga taotletavate õiguspäraste eesmärkide saavutamiseks sobivad ega läheks kaugemale sellest, mis on nende eesmärkide saavutamiseks sobiv ja vajalik“[85]. Seepärast hinnatakse vajalikkust ja proportsionaalsust põhimõtteliselt alati õigusaktis ette nähtud konkreetse meetme alusel.

85. USA ametiasutused on VI lisas täpsustanud, et riigiprokurörid ja föderaalsete uurimisasutuste agendid saavad juurdepääsu organisatsioonide dokumentidele ja muudele registriandmetele „mitut liiki kohustuslike õigusprotsesside kaudu, sealhulgas vandemeeste kogu (*grand jury*) korraldused, halduskorraldused ja läbiotsimismäärused“, ning nad võivad saada enda valdusesse muud teabevahetust „vastavalt föderaalse kriminaalmenetluse raames antud pealtkuulamise volitustele“[86].

---

[83] 12 U.S.C. §§ 3401–3423.

[84] Vt kohtuotsus, Euroopa Kohus, 6. oktoober 2020, La Quadrature du Net ja teised, liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, ECLI:EU:C:2020:791 (edaspidi „Euroopa Liidu Kohtu otsus La Quadrature du Net“), punkt 140. Vt ka andmekaitsenõukogu 11. aprilli 2017. aasta dokument „Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit“ (Isikuandmete kaitse põhiõigust piiravate meetmete vajalikkuse hindamine: töövahend) ja andmekaitsenõukogu suunised „Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data“ (Eraelu ja isikuandmete kaitse põhiõigusi piiravate meetmete proportsionaalsuse hindamine), 19. detsember 2019.

[85] Vt kohtuotsus, Euroopa Kohus, 8. aprill 2014, Digital Rights Ireland, liidetud kohtuasjad C-293/12 ja C-594/12, ECLI:EU:C:2014:238 (edaspidi „Euroopa Liidu Kohtu otsus Digital Rights Ireland“), punkt 46 ja seal viidatud kohtupraktika.

[86] Otsuse eelnõu VI lisa, lk 2.

Lisaks võivad tsiviilametkonnad ja reguleerivad asutused väljastada organisatsioonidele korraldusi „äridokumentide, elektrooniliselt säilitatud teabe või muude materiaalsete objektide kohta“[87]. Ka neid menetlusi on selgitatud otsuse eelnõu põhjendustes 90–93. Andmekaitsenõukogu märgib, et sellega seoses on otsuse eelnõus osutatud positiivsele muutusele elektrooniliselt säilitatud teavet käsitlevas USA kohtupraktikas[88].

86. Samuti on VI lisas täpsustatud, et need õiguslikud menetlused on mittediskrimineerivad ja üldjuhul kasutatakse neid USAs asuvatelt äriühingutelt teabe saamiseks, olenemata sellest, kas nad on USA-ELi andmekaitseraamistiku alusel sertifitseeritud või mitte, ja „sõltumata andmesubjekti kodakondsusest või elukohast“.

87. Peale selle sisaldab VI lisa järeldusi kaitsemeetmete kohta, mis tulenevad USA põhiseaduse neljandast muudatusest, mille kohaselt on õiguskaitseasutustel läbiotsimiseks ja konfiskeerimiseks põhimõtteliselt vaja kohtu määrust, mille saamiseks tuleb tõendada küllaldast alust ja täita täpsusega seotud nõuded, ning milles on osutatud asjaolule, et erandjuhtudel, kui määrust ei nõuta, peavad õiguskaitseasutused juhinduma põhiseaduse neljanda muudatuse kohasest mõistlikkuse põhimõttest[89]. Isik, keda ennast või kelle vara läbi otsitakse, võib vaidlustada ebaseadusliku läbiotsimise teel saadud tõendid või neist tuletatud tõendid, kui neid tõendeid kasutatakse tema vastu kriminaalkohtumenetluses[90].

88. Kokkuvõttes märgib andmekaitsenõukogu, et kriminaalõiguskaitse või avaliku huviga seotud eesmärkidel USA äriühingutelt kaubandusandmete ja muude registriandmete, sealhulgas juurdepääsupiiranguid ja kaitsemeetmeid käsitleva teabe saamiseks kasutatavate uurimisvahendite süsteemi näol on tegemist põhjaliku, aga ka keerulise meetmete süsteemiga, mis muu hulgas kajastab USA valitsuse föderaalset olemust.

89. Seega võib järeldada, et üldiselt vastab USA õiguskaitsealaste uurimismeetmete süsteem seoses põhiõigustega eraelu puutumatusele ja andmekaitsele vajalikkuse ja proportsionaalsuse nõuetele.

3.1.3 Olemas peaks olema sõltumatu järelevalvemehhanism

90. Andmekaitsenõukogu võtab teadmiseks asjaolu, et enamiku otsuse eelnõus ja VI lisas kirjeldatud menetluste puhul on ametiasutustel enne andmetele juurdepääsu saamist vaja kohtu otsust (näiteks kohtu määrust pealtkuulamiseks[91], kohtu määrust jälitustegevuseks föderaalse telefonikõnede pealtkuulamise seaduse alusel[92] ja läbiotsimismäärusi föderaalsete kriminaalmenetluse eeskirjade (Federal Rules of Criminal Procedure) eeskirja 41 alusel[93]). Tundub siiski, et mitte kõigi puhul neist ei ole vaja kohut kaasata. Näiteks võivad tsiviilametkonnad ja reguleerivad asutused „väljastada

[87] Otsuse eelnõu VI lisa, lk 4.
[88] Vt otsuse eelnõu põhjendus 146. 2018. aasta kohtuotsuses kinnitas USA Ülemkohus, et õiguskaitseasutused vajavad läbiotsimismäärust või vabastust läbiotsimismääruse nõudest, et pääseda juurde tugijaamade asukohaandmetele, mis annavad põhjaliku ülevaate kasutaja liikumisest, ning et kasutaja võib sellise teabe puhul põhjendatult eeldada eraelu puutumatust (Timothy Ivory Carpenter *vs.* Ameerika Ühendriigid, nr 16-402, 585 U.S. (2018)).
[89] Vt otsuse eelnõu VI lisa, lk 2.
[90] Vt otsuse eelnõu põhjendus 90.
[91] Vt otsuse eelnõu põhjendus 92.
[92] Vt otsuse eelnõu VI lisa, lk 3.
[93] Vt otsuse eelnõu põhjendus 90 ja VI lisa, lk 3.

korraldusi“[94]. Sellistel juhtudel on aga võimalus teha korralduse põhjendatuse kohtulik järelkontroll, kuivõrd „halduskorralduse saaja [võib] vaidlustada selle korralduse jõustamise kohtus“[95].

91. Lisaks on otsuse eelnõus kirjeldatud mitmesuguste organite tehtavat järelevalvet föderaalsete kriminaalõiguskaitseasutuste üle, alates eraelu puutumatuse ja kodanikuvabaduste ametnike sisekontrollist kuni väliskontrollini, mida teevad peainspektor või USA Kongressi erikomisjonid[96]. Euroopa Komisjon esitab mitmekülgset ja üksikasjalikku teavet ning jõuab üldjuhul arusaadavate järeldusteni. Seetõttu ei hakka andmekaitsenõukogu neid faktilisi järeldusi ja hinnanguid käesolevas arvamuses kordama.

92. Andmekaitsenõukogu märgib olemasoleva teabe põhjal, et seoses õiguskaitseasutuste juurdepääsuga USA äriühingute valduses olevatele andmetele on kehtestatud suhteliselt usaldusväärne sõltumatu järelevalvemehhanism.

3.1.4 Üksikisikule peavad olema kättesaadavad tõhusad õiguskaitsevahendid

93. Euroopa Liidu Kohtu praktika kohaselt peab üksikisikul olema võimalus kasutada oma õiguste teostamiseks tõhusat õiguskaitsevahendit, kui ta leiab, et neid õigusi ei austata või ei ole austatud. Euroopa Liidu Kohus selgitas kohtuotsuses Schrems I, et „õigusakt, milles ei ole õigussubjektile ette nähtud mingit võimalust kasutada õiguskaitsevahendeid, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada, [ei järgi] harta artiklis 47 sätestatud põhiõiguse tõhusale kohtulikule kaitsele põhisisu. Harta artikli 47 esimene lõik nõuab nimelt, et igaühel, kelle liidu õigusega tagatud õigusi või vabadusi rikutakse, on selles artiklis kehtestatud tingimuste kohaselt õigus tõhusale õiguskaitsevahendile kohtus“[97].

94. Otsuse eelnõu[98] ja selle VI lisa sisaldavad täiendavat teavet asjaomastest seadustest tulenevate võimalike õiguskaitsevahendite kohta, mida üksikisikud saavad kasutada juhul, kui avaliku sektori asutused nende andmetele ebaseaduslikult juurde pääsevad.

95. Sellega seoses on komisjoni sõnade kohaselt[99] haldusmenetluse seaduse 5 U.S.C. §-s 702 (Administrative Procedure Act – APA) sätestatud, et isikul, kelle õigusi on ametkonna tegevuse tulemusel rikutud või keda ametkonna tegevus asjaomase seaduse tähenduses on negatiivselt mõjutanud või kahjustanud, õigus seoses selle tegevusega kohtusse pöörduda.

96. Peale selle on salvestatud teabevahetuse seaduses (Stored Communications Act – SCA) (vastu võetud elektroonilise side privaatsuse seaduse (Electronic Communications Privacy Act) II jaotisena) sätestatud, et iga isik, keda on kahjustanud teadliku või tahtliku käitumise tulemusel toimunud asjaomase peatüki mis tahes rikkumine, võib nõuda rikkumise toime pannud isikult või üksuselt (v.a Ameerika Ühendriikidelt) tsiviilhagis asjakohast heastamist[100]. Lisaks võib iga isik, keda on kahjustanud nimetatud peatüki või peatüki 119 tahtlik rikkumine, algatada USA ringkonnakohtus hagi Ameerika Ühendriikide vastu rahalise kahju sissenõudmiseks[101].

---

[94] Vt otsuse eelnõu VI lisa, lk 4, ja põhjendus 91.
[95] Vt otsuse eelnõu VI lisa, lk 4, ja põhjendus 91.
[96] Vt otsuse eelnõu põhjendused 103–106.
[97] Euroopa Liidu Kohtu otsus Schrems I, punkt 95.
[98] Vt otsuse eelnõu põhjendused 107–112.
[99] Vt otsuse eelnõu põhjendus 109.
[100] 18 U.S.C. § 2707.
[101] 18 U.S.C. § 2712.

97. Samuti sisaldab otsuse eelnõu teavet õiguse kohta saada juurdepääs föderaalasutuse andmetele teabevahetuse seaduse (Freedom of Information Act – FOIA)[102] ja mitme muu seaduse alusel, millega antakse üksikisikutele õigus algatada seoses nende isikuandmete töötlemisega hagi USA avaliku sektori asutuse või ametniku vastu, näiteks pealtkuulamisseadus (Wiretap Act), arvutipettuste ja sellealase kuritarvitamise vastane seadus (Computer Fraud and Abuse Act), föderaalne õigusvastaselt tekitatud kahju hüvitamise seadus (Federal Torts Claim Act), finantsandmetega seotud eraelu puutumatuse seadus (Right to Financial Privacy Act) ja õiglase krediidiinfo seadus (Fair Credit Reporting Act)[103].

98. Seepärast tunneb andmekaitsenõukogu heameelt komisjoni esitatud selgituste üle, mis käsitlevad üksikisikute kasutada olevaid õiguskaitsevahendeid. Samuti kutsub andmekaitsenõukogu komisjoni täiendavalt selgitama, kas need õiguskaitsevahendid võimaldavad andmesubjektil „tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada“, nagu on nõudnud Euroopa Liidu Kohus.

3.1.5 Kogutud teabe edasine kasutamine

3.1.5.1 Nende edastatud andmete edasine kasutamine, millele USA õiguskaitseasutused on juurde pääsenud

99. Andmekaitsenõukogu märgib positiivselt, et otsuse eelnõus hinnatakse selliste andmete edasist kasutamist, millele USA õiguskaitseasutused on juurde pääsenud. Andmekaitsenõukogu väljendab aga kahetsust, et esitatud on ainult üks näide selle kohta, millistel alustel saab teavet täiendavalt levitada[104]. Sellega seoses soovitab andmekaitsenõukogu komisjonil otsuse eelnõus täiendavalt selgitada andmete edasise kasutamise suhtes kohaldatavaid põhimõtteid ja kaitsemeetmeid, nagu on tehtud andmekaitseraamistikus Privacy Shield (5 U.S.C. § 552a)[105].

3.1.5.2 Edasisaatmine väljapoole USAd

100. Lisaks märgib andmekaitsenõukogu, et Euroopa Komisjon on viidanud ka andmete edasisaatmisele USA õiguskaitseasutuste poolt kolmandate riikide asutustele, kuid jällegi vaid seoses justiitsministri suunistega FBI USA-siseste operatsioonide kohta (AGG-DOM)[106]. Andmekaitsenõukogu on seisukohal, et selline teave ja hindamine on hädavajalikud, et võimaldada USA õigusraamistiku ja tavadega pakutava kaitse taseme igakülgset hindamist seoses andmete rahvusvahelise avalikustamise ja edasise kasutamisega. Kuna komisjon on esitanud andmete väljapoole USAd edasisaatmise kohta tervikuna vaid ühe piiratud näite, siis kutsub andmekaitsenõukogu komisjoni täiendavalt selgitama USAs õiguskaitse eesmärkidel kogutud ja seejärel muu hulgas rahvusvaheliste lepingute alusel kolmandatele riikidele edastatud isikuandmete edasisaatmise, edasise kasutamise ja avalikustamise suhtes kohaldatavaid eeskirju ja kaitsemeetmeid.

3.2 Andmetele juurdepääs ja nende kasutamine riikliku julgeoleku eesmärkidel

101. Üldise tähelepanekuna tõdeb andmekaitsenõukogu, et riikidele on antud riikliku julgeoleku küsimustes lai kaalutlusruum, mida on tunnistanud ka Euroopa Inimõiguste Kohus. Samuti tuletab

[102] Vt otsuse eelnõu põhjendus 111.
[103] Vt otsuse eelnõu põhjendus 112.
[104] Vt otsuse eelnõu põhjendus 102.
[105] Vt justiitsministri suunised Föderaalse Juurdlusbüroo (FBI) USA-siseste operatsioonide kohta (AGG-DOM), lk 36, jaotise B punkti 1 alapunkt g.
[106] Vt otsuse eelnõu põhjendus 102.

andmekaitsenõukogu meelde, et nagu on rõhutatud tema ajakohastatud soovitustes Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis,[107] on Euroopa Liidu lepingu artikli 6 lõikes 3 sätestatud, et Euroopa inimõiguste konventsioonis kehtestatud põhiõigused on liidu õiguse üldpõhimõtted. Nagu Euroopa Liidu Kohus oma kohtupraktikas aga meelde tuletab, ei kujuta konventsioon seni, kuni EL ei ole sellega ühinenud, ametlikult ELi õiguskorda kuuluvat õigusinstrumenti[108]. Seega tuleb isikuandmete kaitse üldmääruse artiklis 45 nõutud põhiõiguste kaitse tase kindlaks määrata selle määruse sätete põhjal, mille tõlgendamisel võetakse arvesse ELi hartas sätestatud põhiõigusi. Sellest tulenevalt peavad ELi harta artikli 52 lõike 3 kohaselt selles sätestatud õigused, mis vastavad Euroopa inimõiguste konventsiooniga tagatud õigustele, olema sama tähenduse ja ulatusega, nagu Euroopa inimõiguste konventsioonis sätestatud õigused. Seega, nagu Euroopa Liidu Kohus on meelde tuletanud, tuleb arvesse võtta Euroopa Inimõiguste Kohtu praktikat, mis käsitleb ka ELi hartaga ette nähtud õigusi, kui minimaalset kaitsekünnist ELi hartas sätestatud vastavate õiguste tõlgendamisel[109]. Samas on ELi harta artikli 52 lõike 3 viimases lauses märgitud, et „[s]ee säte ei takista liidu õiguses ulatuslikuma kaitse kehtestamist".

102. Seepärast on andmekaitsenõukogu võtnud alljärgnevas hinnangus arvesse Euroopa Inimõiguste Kohtu praktikat, kui ELi hartas, nagu Euroopa Liidu Kohus on seda tõlgendanud, ei ole sätestatud kõrgemat kaitsetaset, millega nähakse ette muud nõuded kui need, mis on kehtestatud Euroopa Inimõiguste Kohtu praktikas.

103. USA õigusraamistikus on mitu õiguslikku vahendit, mis võimaldavad USA luureasutustel andmeid koguda ning neile edaspidi juurde pääseda ja neid töödelda.

104. Nagu Euroopa Komisjon oma otsuse eelnõus meelde tuletab, „võivad USA luureasutused taotleda riikliku julgeoleku eesmärkidel juurdepääsu Ameerika Ühendriikides asuvatele organisatsioonidele edastatud isikuandmetele üksnes seadusega lubatud juhtudel, eelkõige välisluure ja jälitustegevuse seaduse (FISA) ja/või seadusest tulenevate sätete alusel, millega lubatakse juurdepääs riikliku julgeoleku teabenõuete (National Security Letters – NSL) kaudu"[110]. Korralduse 12333 (EO 12333) alusel on „USA luureasutusel samuti võimalus koguda isikuandmeid, mis võivad hõlmata liidu ja Ameerika Ühendriikide vahel edastamisel olevaid andmeid, väljaspool Ameerika Ühendriike"[111].

105. Seoses andmete kogumise erikordadega, eeskätt FISA paragrahviga 702 ja korraldusega EO 12333, on korralduses EO 14086 nüüd kehtestatud uued eeskirjad kaitsemeetmete tõhustamiseks Ameerika Ühendriikide signaaliluurealase tegevuse puhul. Neid üldisi eeskirju kohaldatakse horisontaalselt ning neid „tuleb täiendavalt rakendada asutuse tegevuspõhimõtete ja menetluste kaudu, millega need igapäevast tegevust käsitlevatesse konkreetsetesse suunistesse üle võetakse"[112]. EO 14086 on suuremas osas asendanud presidendi varasema poliitikasuunise nr 28 (edaspidi „PPD-28")[113].

106. Andmete riikliku julgeoleku eesmärgil kogumise, neile juurde pääsemise ja nende edasise töötlemise suhtes kohaldatava õigusraamistiku hindamiseks on seega oluline uurida konkreetset õigusraamistikku, millega on reguleeritud andmete kogumine USAs ja mujal, see tähendab FISA paragrahvi 702 ja korraldust EO 12333, mida iseenesest ei ole alates andmekaitseraamistiku Privacy

[107] Vt andmekaitsenõukogu soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis.
[108] Vt Euroopa Liidu Kohtu otsus Schrems II, punkt 98.
[109] Vt Euroopa Liidu Kohtu otsus La Quadrature du Net, punkt 124.
[110] Vt otsuse eelnõu põhjendus 115.
[111] Vt otsuse eelnõu põhjendus 117.
[112] Vt otsuse eelnõu põhjendus 120.
[113] Selle korraldusega tühistatakse PPD-28, välja arvatud suunise punktid 3 ja 6 ning salastatud lisa, mis jäävad jõusse. Vt presidendi 7. oktoobri 2022. aasta memorandum riikliku julgeoleku kohta.

Shield eelmisest läbivaatamisest muudetud, võttes arvesse asjaolu, et uue korraldusega EO 14086 on ette nähtud kaitsemeetmed, mida tuleb rakendada ka andmete kogumise puhul konkreetsete tekstide, näiteks FISA paragrahvi 702 ja korralduse EO 12333 alusel.

3.2.1 Tagatis A. Töötlemine peab toimuma kooskõlas õigusaktidega ning põhinema selgetel, täpsetel ja ligipääsetavatel eeskirjadel

107. Seoses riikliku julgeoleku eesmärgil andmete kogumise üldise ülesehituse hindamisega soovib andmekaitsenõukogu tuletada meelde esimest neljast nn Euroopa olulisest tagatisest, mille kohaselt peaks töötlemine „põhinema selgetel, täpsetel ja ligipääsetavatel eeskirjadel“[114].

108. Kooskõlas Euroopa Liidu Kohtu väljakujunenud kohtupraktikaga peab isikuandmete kaitse õiguse igasugune piiramine olema sätestatud seaduses ning õiguslikus aluses, mis võimaldab sellesse õigusesse sekkuda, peab olema määratletud, kui ulatuslikult tohib asjaomase õiguse teostamist piirata[115]. Samuti tuletas kohus meelde, et „õigusakt peab olema riigisiseses õiguses õiguslikult siduv“[116]. Sellega seoses on Euroopa Inimõiguste Kohtu praktikas selgitatud, et terminit „seadus“ tuleb mõista selle sisulises, mitte vormilises tähenduses. See võib hõlmata madalama astme õigusaktide ja selliste regulatiivsete meetmete, mille on vastu võtnud kutseorganisatsioonid, kellele seadusandja on delegeerinud sõltumatu õigusloomepädevuse, ning isegi kirjutamata õiguse jõustamist. Selleks, et tegemist oleks „seadusega“, peab õigusnorm olema vähemalt piisavalt ligipääsetav ja piisavalt täpselt sõnastatud[117].

109. Nõutav täpsusaste tuleb kindlaks teha õiguse piiramise ulatuse põhjal[118]. Peale selle tuletas Euroopa Inimõiguste Kohus kohtuotsuses Zakharov meelde, et salajase jälgimise, näiteks sõnumite pealtkuulamise ja -vaatamise kontekstis „ei saa [seaduse] etteaimatavuse nõue tähendada seda, et see peab lubama igaühel ette näha, kas ja millal võivad ametiasutused tema sõnumeid pealt kuulata või vaadata, et ta saaks seega oma tegevust korraldada“. Selged ja üksikasjalikud eeskirjad salajase jälgimise meetmete kohta on aga äärmiselt olulised, et vältida meelevaldsuse ohtu, kui täitevvõimule antud volitusi teostatakse salaja. „Riiklik õigus peab olema piisavalt selge, et anda kodanikele piisavalt teavet selle kohta, millistel asjaoludel ja millistel tingimustel on ametiasutustel õigus selliseid meetmeid kasutada“[119].

110. Peale selle selgitas Euroopa Liidu Kohus, et kolmanda riigi kohaldatava seaduse hindamisel tuleks keskenduda sellele, kas üksikisikud saavad kohtus sellele tugineda. Eelkõige peab olema võimalik andmesubjektidele antud õigustele tugineda ja üksikisikutele tuleb anda avaliku sektori asutuste vastu kohtulikult kaitstavad õigused,[120] mida varasema PPD-28 puhul ei tehtud. Nüüd on korraldusega

---

[114] Soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis (vastu võetud 10. novembril 2020). Vt kohtuotsuse Schrems II punktid 175 ja 180 ning 26. juuli 2017. aasta arvamuse 1/15 (ELi-Kanada broneeringuinfo leping) punkt 139 ja seal viidatud kohtupraktika.

[115] Vt Euroopa Liidu Kohtu otsus Schrems II, punktid 174–175 ja seal viidatud kohtupraktika. Seoses liikmesriikide avaliku sektori asutuste juurdepääsuga vt ka kohtuotsus Privacy International, C-623/17, ECLI:EU:C:2020:790 (edaspidi „Euroopa Liidu Kohtu otsus Privacy International“), punkt 65, ja Euroopa Liidu Kohtu otsus La Quadrature du Net, punkt 175.

[116] Euroopa Liidu Kohtu otsus Privacy International, punkt 68.

[117] Kohtuotsus, Euroopa Inimõiguste Kohus, 26. aprill 1979, Sunday Times *vs.* Ühendkuningriik (nr 1), CE:ECHR:1979:0426JUD000653874 (edaspidi „Euroopa Inimõiguste Kohtu otsus Sunday Times *vs.* Ühendkuningriik nr 1“), punkt 49.

[118] Euroopa Inimõiguste Kohtu otsus Sunday Times *vs.* Ühendkuningriik nr 1, punkt 49.

[119] Kohtuotsus, Euroopa Inimõiguste Kohus, 4. detsember 2015, Zakharov *vs.* Venemaa (edaspidi „Euroopa Inimõiguste Kohtu otsus Zakharov“), punkt 229.

[120] Euroopa Liidu Kohtu otsus Schrems II, punkt 181.

EO 14086, millel andmekaitsenõukogu arusaamise kohaselt peaks olema USA õiguskorras samasugune õiguslik mõju kui suunisel PPD-28 (see tähendab, see on täitevvõimu jaoks siduv), ette nähtud avaliku sektori asutuste vastu kaitstavad õigused. Üksikasjalik hinnang andmesubjektide kohtulikult kaitstavate õiguste kohta on esitatud õiguskaitset käsitlevas jaos.

111. Otsuse eelnõu põhjendustes 114–152 ja VII lisas on esitatud kokkuvõte teatavatest reguleeriva õigusraamistiku, andmete kogumise piirangute, säilitamise ja levitamise piirangute, nõuetele vastavuse ja järelevalve, läbipaistvuse ja õiguskaitse aspektidest. USA luuretegevust käsitlev õigussüsteem koosneb paljudest eri dokumentidest, sealhulgas individuaalsete asutuste aruannetest, tegevuspõhimõtetest ja menetlustest. Sellega seoses keskendutakse andmekaitsenõukogu hinnangus piiratud arvule küsimustele, mida ta peab äärmiselt oluliseks.

112. Otsuse eelnõu põhjenduste 115–119 kohaselt võivad USA riikliku julgeoleku asutused saada juurdepääsu edastatud isikuandmetele üksnes FISA alusel, muude seadusest tulenevate sätete alusel (12 U.S.C. § 3414, 15 U.S.C. § 1681u–1681v ja 18 U.S.C. § 2709) või edastamisel olevate isikuandmete puhul korralduse EO 12333 alusel. Otsuse eelnõu põhjenduste 116 ja 118 kohaselt keskendub komisjon oma hinnangus, mis käsitleb USA riikliku julgeoleku asutuste juurdepääsu isikuandmetele, FISA paragrahvidele 105, 302, 402, 501 ja 702 (väljaspool USAd asuvatele USA-välistele isikutele suunatud välisluuretegevus) ja korraldusele EO 12333 (edastamisel olevate isikuandmetega seotud välisluuretegevus) – sätetele, mis on kõige asjakohasemad. Seepärast piirdub andmekaitsenõukogu oma arvamuses komisjoni hinnanguga nendele sätetele, võttes arvesse korralduses EO 14086 kehtestatud piiranguid ja kaitsemeetmeid[121].

113. Sellega seoses tuleb tähele panna, et kõik otsuse eelnõus nimetatud õigusaktid on üldsusele (nii USAs kui ka mujal) ligipääsetavad ja veebis kättesaadavad. Peale selle on korralduses sätestatud nõuded kogu luureühendusele siduvad[122] ja neid kohaldatakse valdkonnaüleselt kogu välisluure eesmärgil toimuvale tegevusele.

114. Korralduses EO 14086 ei ole mõistet „signaaliluure“ määratletud. Nimetatud korralduses on välisluure ja vastuluure ulatuse kindlaksmääramiseks osutatud korralduses EO 12333 esitatud määratlustele, kus need mõisted on määratletud laialt. Kuigi on väidetud, et pärast FISA kehtestamist saab korraldust EO 12333 kasutada ainult andmete kogumiseks väljaspool USA territooriumi, tuletab andmekaitsenõukogu sellega seoses meelde, et korralduses EO 12333, mida ei muudeta, ei ole esitatud piisavalt üksikasju selle geograafilise kohaldamisala kohta, andmete kogumise, säilitamise või edasise levitamise ulatuse kohta, nende rikkumiste laadi kohta, mida võidakse jälgida, ega selle kohta, mis liiki teavet võidakse koguda või kasutada. Põhimõtteliselt võib igasugune korralduse EO 12333 kohaldamisalasse kuuluv välisluureandmete kogumine toimuda USA presidendi kaalutlusõiguse põhjal[123]. Andmekaitsenõukogu arusaamise kohaselt on aga EO 14086 põhieesmärk kehtestada välisluure kontekstis toimuva isikuandmete kogumise ja töötlemise piirangud, olenemata sellest, millist jälitustegevuse programmi kasutatakse ja kust andmeid saadakse. Seepärast saab andmekaitsenõukogu olukorrast aru nii, et EO 14086 raames ette nähtud täiendavad kaitsemeetmed

121 Selle korraldusega tühistatakse PPD-28, välja arvatud suunise punktid 3 ja 6 ning salastatud lisa, mis jäävad jõusse. Vt presidendi 7. oktoobri 2022. aasta memorandum riikliku julgeoleku kohta.
122 Vt otsuse eelnõu põhjendus 120.
123 USA põhiseaduse II artikli alusel vastutab riikliku julgeoleku tagamise, sealhulgas eeskätt välisluureandmete kogumise eest president kui relvajõudude ülemjuhataja.

on kohaldatavad ka EO 12333 alusel edastavate isikuandmete suhtes kohaldatavate jälitustegevuse programmide puhul[124].

115. Sellega seoses on korralduses EO 14086 loetletud 12 seaduslikku eesmärki, mida tuleks signaaliluureandmete kogumisel täita, ja viis eesmärki, milleks signaaliluureandmeid ei tohi koguda,[125] samuti kuus seaduslikku eesmärki laiaulatuslikult kogutud andmete kasutamiseks[126]. Osad neist on küll suhteliselt üksikasjalikud (näiteks „pantvangide vabastamine"), teised aga üldisemad (näiteks „ülemaailmne julgeolek"). Korralduses EO 14086 on sätestatud ka loetelu keelatud eesmärkidest, mis hõlmavad eelkõige „seaduslike eraelu puutumatusega seotud huvide" allasurumist või piiramist[127]. Samuti on korraldusega EO 14086 Ameerika Ühendriikide presidendile ette nähtud võimalus lisada loetelusse muid eesmärke, milleks kogumist lubatakse ja mida ei pruugita presidendi otsuse põhjal avalikustada, kui president leiab, et see ohustaks Ameerika Ühendriikide julgeolekut[128]. Sellised ajakohastused võivad olla lubatud üksnes „uute riikliku julgeolekuga seotud tungivate vajaduste" tekkimisel.

116. Luureasutused ei saa signaaliluureandmete kogumise õigustusena tugineda eesmärkidele endile, vaid operatiiveesmärke silmas pidades peab täiendavalt põhjendama signaaliluureandmete kogumist konkreetsemate prioriteetidega, milleks neid andmeid võib koguda. Korralduses EO 14086 on üksikasjalikult kirjeldatud nende prioriteetide kinnitamise menetlust, milleks signaaliluureandmeid võib koguda[129]. Andmekaitsenõukogu saab sellest aru nii, et kinnitatud luureprioriteetide määratlemise protsessi eest vastutab põhimõtteliselt luureühenduse direktor (Director of the Intelligence Community), ja tunnistab, et reeglina peaks see hõlmama riikliku luurejuhi ameti (Office of the Director of National Intelligence) kodanikuvabaduste kaitse ametniku (Civil Liberties Protection Officer – CLPO) hinnangut, millega direktor võib mitte nõustuda, millisel juhul „hõlmab see riikliku luureprioriteetide raamistiku (National Intelligence Priorities Framework – NIPF) presidendile esitamisel CLPO hinnangut ja direktori seisukohti"[130].

117. Andmekaitsenõukogu märgib aga ühtlasi, et vastavalt „kinnitatud luureprioriteetide" määratlusele tähendavad need prioriteedid „enamiku USA signaaliluureandmete kogumise alase tegevuse" puhul[131] korralduse § 2(b)(iii) (mida on kirjeldatud eelmises punktis) alusel kinnitatud prioriteete. „Piiratud asjaoludel" võib kinnitamismenetlus sellest protsessist erineda, millisel juhul president või luureühenduse liikme juht võib kehtestada prioriteedi „mõistlikus ulatuses" kooskõlas § 2(b)(iii)(A)(1)–(3) sätestatud kriteeriumidega, mis hõlmavad nõuet võtta sobilikult arvesse kõikide isikute eraelu puutumatust ja kodanikuvabadusi, kuid sellesse menetlusse ei kaasata CLPOd.

118. Lisaks on korralduses EO 14086 rõhutatud, et „signaaliluureandmete kogumise alane tegevus on kohandatud sel määral, mis on mõistlik" luureprioriteedi edendamiseks, ning et „luureühendus kaalub muude vähem sekkuvate allikate kättesaadavust, mõistlikkust ja asjakohasust" ning esitab üldised nõuded seoses vajalikkuse ja proportsionaalsuse põhimõtetega[132].

[124] Vt otsuse eelnõu põhjendus 134.
[125] Vt korraldus 14086 (EO 14086), § 2(b)(ii)(A)(1)–(5).
[126] Vt otsuse eelnõu põhjendus 134 ja korraldus EO 14086, § 2(c)(ii).
[127] Vt korraldus EO 14086, § 2(b)(ii)(A)(2).
[128] Vt korraldus EO 14086, § 2(b)(i)(B).
[129] Vt otsuse eelnõu põhjendus 129.
[130] Vt korraldus EO 14086, § 2(b)(iii)(B).
[131] Vt korraldus EO 14086, § 4(n).
[132] Vt korraldus EO 14086, § 2(c)(i)(A) ja (B).

119. Peale selle kehtestatakse korraldusega EO 14086 selle 5. jao punkti h kohaselt õigus esitada CLPO-le vastavust käsitlevaid kaebusi ja lasta andmekaitseasju läbivaataval kohtul CLPO otsused kooskõlas korralduse 3. jaos kehtestatud õiguskaitsemehhanismiga läbi vaadata.

120. Seoses luureoperatsioonidega, mida võidakse lubada, tundub FISA tekst olevat EO 12333 omast selgem ja täpsem. Praegu tuleb FISA ja EO 12333 kohaldamisel arvestada korraldust EO 14086 ning võtta muu hulgas eelkõige arvesse vajalikkuse ja proportsionaalsuse põhimõtteid.

121. Korralduses EO 14086 sätestatud nõudeid tuleb täiendavalt rakendada asutuse tegevuspõhimõtetes ja menetlustes, millega need igapäevast tegevust käsitlevatesse konkreetsetesse suunistesse üle võetakse. Sellega seoses on USA luureasutustele korraldusega EO 14086 antud maksimaalselt üks aasta oma olemasolevate tegevuspõhimõtete ja menetluste ajakohastamiseks ning korralduses kehtestatud nõuetega kooskõlla viimiseks (see tähendab 7. oktoobrini 2023). Nende ajakohastatud tegevuspõhimõtete ja menetluste väljatöötamisel tuleb konsulteerida justiitsministri, CLPO ning eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoniga (Privacy and Civil Liberties Oversight Board – PCLOB) ning need tuleb võimalikult suurel määral avalikult kättesaadavaks teha[133].

122. Andmekaitsenõukogu pooldaks olukorda, kus mitte üksnes otsuse jõustumine, vaid ka selle vastuvõtmine sõltuvad sellest, et muu hulgas võtavad kõik USA luureasutused vastu ajakohastatud poliitika ja menetlused EO 14086 rakendamiseks. Andmekaitsenõukogu soovitab komisjonil hinnata seda ajakohastatud poliitikat ja neid menetlusi ning jagada seda hinnangut andmekaitsenõukoguga.

123. Seoses edastatud ja riikliku julgeoleku eesmärgil kogutud andmete säilitamisega märgib andmekaitsenõukogu, et korraldusega EO 14086 tagatakse USA isikute isikuandmete suhtes kohaldatavate eeskirjade kohaldatavus ka USA-väliste isikute isikuandmete suhtes[134]. Otsuse eelnõust ilmneb, et need eeskirjad on sätestatud 2015. eelarveaastaks vastu võetud luure volitamise seaduse (Intelligence Authorization Act) paragrahvis 309,[135] kus on põhimõtteliselt kehtestatud viie aasta pikkune säilitamisperiood kogu mitteavaliku telefoni- või elektroonilise side andmetele, mis on saadud ilma isiku nõusolekuta. Sellega seoses soovitab andmekaitsenõukogu komisjonil selgitada otsuses lähemalt oma hinnangut USA isikute isikuandmete suhtes kohaldavate säilitamiseeskirjade kohta.

3.2.2 Tagatis B. Taotletavate seaduslike eesmärkide vajalikkust ja proportsionaalsust on vaja tõendada

3.2.2.1 Uue korraldusega 14086 ette nähtud horisontaalsete kaitsemeetmete vajalikkus ja proportsionaalsus

124. Uue korralduse EO 14086, millega üldiselt asendati PPD-28, eesmärk on näha ette Ameerika Ühendriikide signaaliluurealase tegevusega seotud kaitsemeetmete tõhustamise eeskirjad, mida luureühenduse liikmed oma sisemenetlustes ja tegevuspõhimõtetes täiendavalt rakendavad.

125. Korraldusega EO 14086 kehtestatakse USA õiguse alusel kaks uut nõuet, mis kajastavad nõudeid, mida Euroopa Liidu Kohus tuletas meelde kohtuotsuses Schrems II, nimelt et signaaliluurega seotud tegevust viiakse ellu ainult sel määral, mil see on vajalik kinnitatud luureandmete prioriteetse

[133] Vt korraldus EO 14086, § 2(c)(iv)(B) ja (C).
[134] Otsuse eelnõu põhjendus 150.
[135] Otsuse eelnõu põhjendus 272.

kogumise soodustamiseks, ning üksnes selles ulatuses ja sel viisil, mis on proportsionaalne kinnitatud luureandmete prioriteetsusega[136].

126. Andmekaitsenõukogu arusaamise kohaselt on need elemendid hõlmatud selleks, et kajastada ELi õiguse alusel ning Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu praktikas ette nähtud vajalikkuse ja proportsionaalsuse põhimõtteid, mille eesmärk on tagada andmete kogumise ja töötlemise piiramine vajaliku ja proportsionaalsega.

127. Sellega seoses tuletab andmekaitsenõukogu meelde nii luureprioriteetide kinnitamiseks ette nähtud menetlust kui ka selle võimalikku erandit (vt punktid 116 ja 117).

128. Lisaks märgib andmekaitsenõukogu, et need korralduses kehtestatud vajalikkuse ja proportsionaalsuse põhimõtted tuleb ühe aasta jooksul kasutusele võtta ja rakendada luureühenduse kõikide liikmete tegevuspõhimõtetes ja menetlustes[137].

3.2.2.2 Konkreetsed kaitsemeetmed seoses signaaliluureandmete kogumisega

129. Samuti märgib andmekaitsenõukogu, et korraldusega EO 14086 nähakse seoses signaaliluureandmete kogumisega ette nende eesmärkide piirangud, milleks isikuandmeid võib ja ei tohi koguda[138].

130. Andmekaitsenõukogu tunneb heameelt asjaolu üle, et korralduse kohaselt tuleb andmete laiaulatuslikule kogumisele eelistada sihipärast kogumist[139]. Seoses signaaliluureandmete kogumisega on korralduses esitatud loetelu 12 eesmärgist, milleks andmeid võib koguda ja mida tuleb täiendavalt põhjendada luureprioriteetidega (vt punkt 117), ning loetelu viiest eesmärgist, milleks signaaliluureandmeid ei tohi koguda[140]. Põhimõtteliselt tagatakse nende sätetega andmete kogumise vajalikkus.

131. Andmekaitsenõukogu tuletab siiski meelde, et korraldusega EO 14086 on Ameerika Ühendriikide presidendile ette nähtud võimalus lisada loetelusse muid eesmärke (vt punktid 114 ja 115)[141].

3.2.2.3 Konkreetsed kaitsemeetmed seoses andmete laiaulatusliku kogumisega

132. Euroopa Liidu Kohus rõhutas kohtuotsuses Schrems I, et „eraelu puutumatuse põhiõiguse kaitsmine liidu tasandil [nõuab], et isikuandmete kaitse erandid ja piirangud piirduksid rangelt vajalikuga“,[142] ning otsustas, et „õigusakti, mis võimaldab ametiasutustel elektroonilise side sisuga üldiselt tutvuda, [tuleb] pidada harta artikliga 7 tagatud eraelu puutumatuse põhiõiguse põhisisu kahjustavaks“.

133. Nagu eespool meelde tuletatud, rõhutas kohus kohtuotsuses Schrems II[143] oma analüüsis laiaulatusliku kogumise kohta seoses korralduse EO 12333 ja suunise PPD-28 koostoimes lugemisega ning eriti punktides 183–185, et andmete laiaulatusliku kogumise võimalus, mis võimaldab „pääseda korraldusel EO 12333 põhinevate jälgimisprogrammide raames juurde USAsse liikuvatele andmetele, ilma et selle juurdepääsu suhtes toimuks mingitki kohtulikku kontrolli, ei sea igal juhul piisavalt selgelt ja täpselt piire isikuandmete sellisele laiaulatuslikule kogumisele“.

[136] Vt korraldus EO 14086, § 2(a)(ii)(A) ja (B).
[137] Vt korraldus EO 14086, § 2(c)(iv)(B).
[138] Vt korraldus EO 14086, § 2(b)(i)(A)(1)–(12).
[139] Vt korraldus EO 14086, § 2(c)(ii)(A).
[140] Vt korraldus EO 14086, § 2(b)(ii)(A)(1)–(5)
[141] Vt korraldus EO 14086, § 2(b)(i)B).
[142] Euroopa Liidu Kohtu otsus Schrems I, punkt 92.
[143] Vt Euroopa Liidu Kohtu otsus Schrems II.

134. Seega märgib andmekaitsenõukogu, et Euroopa Liidu Kohus ei välistanud põhimõtteliselt andmete laiaulatuslikku kogumist, kuid leidis kohtuotsuses Schrems II, et selleks, et kõnealune laiaulatuslik kogumine toimuks õiguspäraselt, tuleb sellise laiaulatusliku kogumise piiritlemiseks kehtestada piisavalt selged ja täpsed piirid.

135. Samuti tunnistab andmekaitsenõukogu, et kuigi korraldusega EO 14086 asendatakse PPD-28, nähakse sellega ette uued kaitsemeetmed ja piirangud väljaspool USAd andmete kogumiseks ja kogutud andmete kasutamiseks, sest FISA või konkreetsemate USA seaduste piiranguid ei kohaldata.

136. Seoses andmete laiaulatusliku kogumisega märgib andmekaitsenõukogu, et korralduse EO 14086 alusel on laiaulatuslik kogumine jätkuvalt lubatud. Andmekaitsenõukogu rõhutab, et andmete laiaulatusliku kogumise määratlus on tõepoolest sama kui varasemas suunises PPD-28: „signaaliluure andmete laiaulatuslik kogumine tähendab suure koguse signaaliluure andmete heakskiidetud kogumist, mis tehnilistel või operatiivsetel kaalutlustel toimub ilma kategooriate (näiteks eritunnuste või valikute) kasutamiseta“[144].

137. Alates kohtuotsusest Schrems II ei ole Euroopa Liidu Kohus üksikasjalikult täpsustanud andmete laiaulatuslikuks kogumiseks nõutavaid kaitsemeetmeid. Andmekaitsenõukogu tuletab aga meelde, et Euroopa Inimõiguste Kohus on teinud olulisi otsuseid andmete laiaulatusliku kogumise ja sellega seotud asjakohaste kaitsemeetmete kohta.

138. Andmekaitsenõukogu tuletab meelde, et laiaulatuslik kogumine, mis võimaldab valimatult koguda suurel hulgal andmeid, kujutab üksikisikutele suuremat ohtu[145] kui sihipärane kogumine ja seega tuleb selle puhul tõendada täiendavate kaitsemeetmete olemasolu.

139. Samuti märgib andmekaitsenõukogu, et Euroopa Liidu Kohus on töötanud välja täiendava kohtupraktika seoses liiklus- ja asukohaandmetega ning edasise juurdepääsuga nendele telekommunikatsioonivõrgu operaatorite säilitatavatele andmetele, muu hulgas riikliku julgeoleku eesmärkidel, mida ei saa küll pidada praeguses kontekstis otseselt kohaldatavaks, kuid mis võib olla korralduse EO 12333 raames toimuva andmete laiaulatusliku kogumise käesoleva hindamisel puhul teataval määral asjakohane.

1) <u>Eesmärgi piirang</u>

140. Korralduses on sätestatud, et laiaulatuslik kogumine peaks toimuma üksnes pärast seda, kui on kindlaks tehtud, et „kinnitatud luureprioriteedi edendamiseks vajalikku teavet ei ole mõistlikult võimalik saada sihipärase kogumise teel“[146] ning et „luureühenduse liige kohaldab mõistlikke meetodeid ja tehnilisi meetmeid, et piirata kogutud andmeid sellega, mis on vajalik kinnitatud luureprioriteedi edendamiseks, minimeerides samal ajal mitteasjakohase teabe kogumist“[147]. Lisaks nendele kaitsemeetmetele tunnistab andmekaitsenõukogu ka asjaolu, et laiaulatuslikult kogutud andmeid kasutatakse ka selleks, et täita ühte või mitut kuuest loetletud eesmärgist[148]. Samuti rõhutab andmekaitsenõukogu, et kuigi need eesmärgid on üksikasjalikumad kui eelmises suunises PPD-28 (mis

[144] Vt korraldus EO 14086, § 4(b).
[145] Vt nt kohtuotsus, Euroopa Inimõiguse Kohus (suurkoda), 25. mai 2021, Big Brother Watch ja teised *vs.* Ühendkuningriik (edaspidi „Euroopa Inimõiguste Kohtu otsus Big Brother Watch“), põhjendus 363, kus kohus märgib, et „ei väideta, et seotud sideandmete hankimine laiaulatusliku pealtkuulamise ja -vaatamise teel on tingimata vähem sekkuv kui sisu hankimine“.
[146] Korraldus EO 14086, § 2(c)(ii)(A).
[147] Korraldus EO 14086, § 2(c)(ii)(A).
[148] Korraldus EO 14086, § 2(c)(ii)(B).

üldiselt asendati korraldusega EO 14086) sätestatud, siis on sellise andmete kogumise ulatus endiselt lai, mis tähendab, et see hõlmab suurel hulgal andmeid.

141. Andmekaitsenõukogu tuletab ka siinkohal meelde, et korraldusega EO 14086 on Ameerika Ühendriikide presidendile ette nähtud võimalus lisada loetelusse muid eesmärke (vt punkt 115)[149].

2) Eelnev sõltumatu luba

142. Andmekaitsenõukogu rõhutab, et Euroopa Inimõiguste Kohus peab äärmiselt oluliseks eelneva sõltumatu loa andmist andmete laiaulatuslikuks kogumiseks riikliku julgeoleku eesmärkidel. Kohus sedastas eelkõige järgmist: „[K]ohus leiab, et laiaulatusliku pealtkuulamise ja -vaatamise volituste kuritarvitamise ohu minimeerimiseks peavad protsessi suhtes kehtima n-ö läbivad kaitsemeetmed, mis tähendab seda, et riigi tasandil tuleb protsessi igas etapis hinnata võetavate meetmete vajalikkust ja proportsionaalsust, et laiaulatuslikuks pealtkuulamiseks ja -vaatamiseks peab olema sõltumatu luba alates sellest, kui määratletakse toimingu eesmärk ja ulatus, ning et toimingu üle tuleb teha järelevalvet ja sõltumatut sisulist järelhindamist. Kohus leiab, et need on põhilised kaitsemeetmed, millele igasugune artiklile 8 vastav laiaulatusliku pealtkuulamise ja -vaatamise kord peab tuginema".[150]

143. Samuti juhib andmekaitsenõukogu tähelepanu suurkoja kõnealuse otsuse järgmisele punktile, milles Euroopa Inimõiguste Kohus täiendavalt rõhutab, et ta „nõustub koja otsusega, mille kohaselt kohtu luba on küll „oluline kaitsemeede meelevaldsuse vastu", kuid see ei ole „vajalik nõue" (vt koja otsuse punktid 318–320). Sellest hoolimata peaks laiaulatuslikuks pealtkuulamiseks ja -vaatamiseks andma loa sõltumatu organ, see tähendab organ, mis ei sõltu täitevvõimust"[151].

144. Sellega seoses märgib andmekaitsenõukogu, et korralduses ei ole andmete laiaulatuslikuks kogumiseks sellist eelneva sõltumatu loa nõuet kehtestatud, samuti ei ole seda ette nähtud korralduse EO 12333 alusel (vt korraldust EO 12333 käsitlev punkt allpool).

3) Säilitamiseeskirjad

145. Andmekaitsenõukogu tuletab meelde, et veel üks oluline kaitsemeetmete kogum on andmete kogumise ja säilitamise kestust käsitlevad eeskirjad. Selles küsimuses rõhutas Euroopa Inimõiguste Kohus, et „riigi õiguses tuleks kehtestada pealtkuulamise ja -vaatamise kestuse piirang, menetlus, mida tuleb saadud andmete kontrollimisel, kasutamisel ja säilitamisel järgida, ettevaatusabinõud, mida tuleb andmete teistele isikutele edastamisel võtta, ning asjaolud, mille korral võib pealtkuulamise ja -vaatamise teel saadud andmeid kustutada või hävitada" või peab seda tegema,[152] sest need kaitsemeetmed „on samavõrd olulised laiaulatusliku pealtkuulamise ja -vaatamise puhul"[153].

146. Andmekaitsenõukogu mõistab seda nii, et korraldusega nähakse ette eeskirjad signaaliluure kaudu (sealhulgas laiaulatuslikult) kogutud isikuandmete säilitamise kohta[154]. Andmekaitsenõukogu märgib, et korralduse EO 14086 § 2(c)(iii)(A) kohaselt peab iga luureühenduse liige, kes signaaliluure kaudu kogutud isikuandmeid menetleb, kehtestama ja kohaldama tegevuspõhimõtteid ja menetlusi, mille eesmärk on minimeerida signaaliluure kaudu kogutud isikuandmete levitamist ja säilitamist. Nendes eeskirjades ei ole aga kehtestatud konkreetset säilitamisperioodi, vaid on üldiselt osutatud samadele

[149] Vt korraldus EO 14086, § 2(c)(ii)(C).
[150] Vt Euroopa Inimõiguste Kohtu otsus Big Brother Watch, punkt 350.
[151] Vt Euroopa Inimõiguste Kohtu otsus Big Brother Watch, punkt 351.
[152] Vt Euroopa Inimõiguste Kohtu otsus Big Brother Watch, punkt 348.
[153] Vt Euroopa Inimõiguste Kohtu otsus Big Brother Watch, punkt 348.
[154] Vt korraldus EO 14086, § 2(c)(iii)(A)(2)(a)–(c).

kohaldatavatele eeskirjadele, mis kehtivad USA isikuid käsitlevate andmete säilitamise puhul, ja olukordadele, kus ei ole andmete säilitamise kohta lõplikku otsust tehtud. Seega tunneb andmekaitsenõukogu muret selle pärast, et sarnaselt sihipärasele andmete kogumisele (vt punkt 122) ei ole kõnealused laiaulatuslikult kogutud andmete säilitamise perioodid selles korralduses selgelt määratletud. Andmekaitsenõukogu kutsub komisjoni jagama oma hinnangut USA isikute suhtes kohaldatavate säilitamisperioodide vajalikkuse ja proportsionaalsuse kohta ning kättesaadavat teavet praktikas järgitavate säilitamisperioodide kohta juhul, kui USA õiguse alusel ei ole tehtud säilitamist käsitlevat lõplikku otsust, sest praegusel kujul on otsuse eelnõus seda üldreeglit üksnes meelde tuletatud ühes lühikeses punktis[155] ja joonealuses märkuses,[156] mis ei võimalda kindlaks teha, kas need säilitamisperioodid on vajalikud ja proportsionaalsed. Nagu Euroopa Inimõiguste Kohus on rõhutanud, on see andmesubjektide jaoks äärmiselt oluline kaitsemeede, mis võimaldab neil teostada oma õigusi juhul, kui nende andmete algseks kogumiseks võetakse eriti sekkuvaid meetmeid. Seega kutsub andmekaitsenõukogu Euroopa Komisjoni täiendavalt selgitama erinevaid säilitamisperioode, mida tegelikult järgitakse.

4) <u>Levitamisega seotud kaitsemeetmed</u>

147. Samuti tuletab andmekaitsenõukogu meelde, et Euroopa Inimõiguste Kohus tunnistas, et vajalikkuse ja proportsionaalsuse ning eesmärgi piiramise põhimõtte tulemuslikkuse tagamisel on olulised ka seadusega ette nähtud normid kogutud andmete edasise levitamise kohta, sealhulgas laiaulatusliku kogumise puhul[157].

148. Korralduses EO 14086 (§ 2(c)(iii)(A)(1)(c)) on sätestatud, et signaaliluurealase tegevuse kaudu kogutud teavet USA-väliste isikute kohta tohib levitada ainult juhul, kui volitatud ja asjakohast koolitust saanud isikul on mõistlik alus arvata, et isikuandmeid kaitstakse nõuetekohaselt, ja kui see teave on saajale vajalik.

149. Seda arvesse võttes mõistab andmekaitsenõukogu, et mis puudutab andmete levitamist USA pädevatele asutustele, siis ei ole korralduse EO 14086 kohaste levitamist käsitlevate sätetega ette nähtud sõnaselget levitamise keeldu muudel otstarvetel kui riikliku julgeoleku eesmärgil[158]. Andmekaitsenõukogu kutsub komisjoni täiendavalt selgitama sellisel juhul kohaldatavaid eeskirju ja kaitsemeetmeid.

150. Seepärast tunneb andmekaitsenõukogu muret, et luureühenduse pädevate asutuste hangitud teavet võidakse levitada USA pädevatele asutustele kuritegevuse, sealhulgas raskete kuritegude vastu võitlemiseks kriminaaluurimiste käigus, andes seega õiguskaitseasutustele ilma täiendavate konkreetsete piiranguteta võimaluse saada andmeid, mida neil oleks keelatud otse koguda, ning kutsub komisjoni seda küsimust täiendavalt hindama.

151. Seoses konkreetselt edasisaatmisega (andmete levitamine vastuvõtjatele väljaspool Ameerika Ühendriikide valitsust, sealhulgas välisriigi valitsusele või rahvusvahelisele organisatsioonile[159]) tuletab

[155] Vt otsuse eelnõu punkt 150.
[156] Vt otsuse eelnõu joonealune märkus nr 271.
[157] Vt Euroopa Inimõiguste Kohtu otsus Big Brother Watch, punkt 348.
[158] Vt korraldus EO 14086, § 2(c)(iii)(A)(1).
[159] Vt korraldus EO 14086, eelkõige § 2(c)(iii)(A)(1)(d).

andmekaitsenõukogu meelde, et tema arvamuse kohaselt tuleb andmetele tagatud kaitse säilitada ka edasisaatmise puhul, sealhulgas riikliku julgeoleku valdkonnas[160].

152. Sellega seoses on korraldusega ette nähtud teatavad kaitsemeetmed, nimelt nõue võtta nõuetekohaselt arvesse levitamise eesmärki – kuigi sõnaselgelt ei ole nõutud, et ka levitamise eesmärk peab olema riikliku julgeoleku kaitse –, levitatavate isikuandmete laadi ja ulatust ning võimalikku kahjulikku mõju asjaomas(t)ele isiku(te)le enne andmete levitamist.

153. Kuigi andmekaitsenõukogu tunnistab, et mõned nendest kaitsemeetmetest, eelkõige nõue võtta arvesse võimalikku kahjulikku mõju[161] asjaomas(t)ele andmesubjekti(de)le, kajastavad mõningaid Euroopa Inimõiguste Kohtu kehtestatud nõudeid, rõhutab ta samuti, et Euroopa Inimõiguste Kohus nõuab ka õiguslikult siduvat kohustust „analüüsida ja teha kindlaks, kas luureandmete vastuvõtja välisriigis pakub vastuvõetaval minimaalsel tasemel kaitsemeetmeid“,[162] mida andmekaitsenõukogu andmete välisriigis asuvale vastuvõtjale levitamist käsitlevates korralduse sätetes sõnaselgelt ei tuvastanud. Seepärast kutsub andmekaitsenõukogu komisjoni seda elementi täiendavalt hindama.

154. Euroopa Andmekaitsenõukogu märgib ka seda, et Euroopa Komisjon ei võtnud kaitse piisavuse hindamisel arvesse kolmandate riikide või rahvusvaheliste organisatsioonidega sõlmitud rahvusvahelisi lepinguid, millega võidakse ette näha erisätted isikuandmete rahvusvahelise edastamiseks luureteenistustelt kolmandatele riikidele. Andmekaitsenõukogu leiab, et kolmandate riikidega tehtavat luurekoostööd käsitlevate kahe- või mitmepoolsete lepingute sõlmimine tõenäoliselt mõjutab hinnatud andmekaitseraamistikku.

155. Seepärast kutsub andmekaitsenõukogu Euroopa Komisjoni selgitama välja, kas sellised lepingud on olemas ja millistel tingimustel saab neid sõlmida, ning hindama, kas rahvusvaheliste lepingute sätted võivad mõjutada EMPst edastatud isikuandmetele õigusraamistiku ja tavade abil tagatava kaitse taset seoses riikliku julgeoleku eesmärkidel edasisaatmisega.

5) <u>Andmete ajutine laiaulatuslik kogumine sihipärase kogumise algse tehnilise etapi toetamiseks</u>

156. Andmekaitsenõukogu tuletab meelde, et andmekaitseraamistiku Privacy Shield viimase ühise läbivaatamise ajal keskenduti aruteludes peamiselt sellele, kuidas tõlgendada ja kohaldada andmete laiaulatusliku kogumise täiendavat alust (olukord/stsenaarium), mis on ette nähtud PPD-28 2. jao joonealuse märkuse nr 5 esimese lausega, mille kohaselt „[k]äesolevas jaos sisalduvaid piiranguid ei kohaldata signaaliluureandmete suhtes, mida kogutakse ajutiselt andmete sihipärase kogumise hõlbustamiseks“. USA ametiasutused selgitasid asjaomasel ajal, mida „signaaliluureandmed, mida kogutakse ajutiselt andmete sihipärase kogumise hõlbustamiseks“ tähendab. Andmekaitsenõukogu sai nende arutelude põhjal aru nii, et kõnealuse joonealuse märkuse kohaselt tohib andmeid laiaulatuslikult koguda – olenemata kuuest ettenähtud eesmärgist – siis, kui seda tehakse ajutise eesmärgiga määrata kindlaks tuvastatud objekti tunnused. Seega oleks tegemist täiendava alusega andmete laiaulatuslikuks kogumiseks ja sellisel juhul kohaldataks jätkuvalt ainult PPD-28 1. jao üldpõhimõtteid. Nagu eespool meelde tuletati, oli Euroopa Liidu Kohus kohtuotsuses Schrems II

[160] Vt nt andmekaitsenõukogu arvamus 14/2021 Euroopa Komisjoni määruse (EL) 2016/679 kohase rakendusotsuse eelnõu kohta, mis käsitleb isikuandmete piisavat kaitset Ühendkuningriigis (vastu võetud 13. aprillil 2021), punktid 4.3.2.1 ja 4.3.2.2.

[161] Vt korraldus EO 14086, § 2(c)(iii)(A)(1)(d).

[162] Vt kohtuotsus, Euroopa Inimõiguste Kohus (suurkoda), 25. mai 2021, Centrum För Rättvisa *vs.* Rootsi, punkt 326.

seisukohal, et seoses andmete laiaulatusliku kogumisega ei sea EO 12333 ja PPD-28 üheskoos „piisavalt selgelt ja täpselt piire isikuandmete sellisele laiaulatuslikule kogumisele“[163].

157. Andmekaitsenõukogu märgib, et ka korralduses EO 14086 on sätestatud seda laadi laiaulatuslikku kogumist võimaldav erand;[164] andmekaitsenõukogu tunneb aga heameelt selle üle, et võrreldes suunisega PPD-28 on seda erandit kitsendatud, ning samuti korralduse EO 14086 alusel tagatud täiendavate kaitsemeetmete üle.

158. Andmekaitsenõukogu arusaamise kohaselt nähakse uue korraldusega EO 14086 ette kaitsemeetmed, mida seda laadi ajutise tehnilise laiaulatusliku kogumise suhtes jätkuvalt kohaldatakse, eelkõige üldpõhimõtted vajalikkuse ja proportsionaalsuse kohta võrreldes kinnitatud luureprioriteediga, kui andmeid kogutakse kategooriaid kasutamata enne sihipärast kogumise toimumist (vt korraldus EO 14086, § 2(a)–(b), § 2(c)(i)). Samuti saab andmekaitsenõukogu aru nii, et sellise laiaulatusliku kogumise suhtes, mis toetab järgnevat sihipärast signaaliluureandmete kogumist, kohaldatakse samuti täiendavaid kaitsemeetmeid, mis on sätestatud alajaotise 2 punkti c alapunktis iii ja järgmistes alapunktides[165].

159. Andmekaitsenõukogu tuletab aga samuti meelde, et mõiste „kinnitatud luureprioriteet“ määratlusega on ette nähtud erandlik menetlus, millesse ei ole kaasatud riikliku luurejuhi ameti CLPOd.

160. Andmekaitsenõukogu märgib siiski, et laiaulatuslikku kogumist käsitlevas alajaotises esitatud kaitsemeetmeid ei kohaldata ajutise laiaulatusliku kogumise suhtes, mis toetab sihipärase signaaliluuretegevuse esialgset tehnilist etappi, nagu on kirjeldatud korralduse EO 14086 §-s 2(c)(ii)(D), mis tähendab eelkõige seda, et sellises olukorras laiaulatuslikult kogutud andmeid saab kasutada muudel eesmärkidel kui need, mis on loetletud §-s 2(c)(ii). Andmekaitsenõukogu soovib otsuse eelnõus näha täiendavaid selgitusi eesmärkide kohta, milleks sellises olukorras laiaulatuslikult kogutud andmeid saab kasutada, ja seoses piirangute kohaldamisega, mis on sätestatud §-s 2(c)(i) ajutise laiaulatusliku kogumise raames signaaliluureandmete üldise kogumise suhtes (täpsemalt üksnes seal loetletud seaduslikel eesmärkidel).

161. Lõpetuseks rõhutab andmekaitsenõukogu ka seda, et ebaselgeks jäävad kõnealune erand andmete laiaulatusliku kogumise kohta sihipärase kogumise eesmärgil ja ülejäänud kaitsemeetmed, mida tuleb kohaldada, eelkõige see, milliseid korralduses EO 14086 sätestatud kaitsemeetmeid mis etapis (laiaulatuslik kogumine, täiendav sihipärane kogumine) kohaldatakse, ning kutsub komisjoni neid elemente täiendavalt hindama, samuti hindama tulevastes ühistes läbivaatamistes nende aspektide tegelikku rakendamist.

162. Peale selle tunneb andmekaitsenõukogu kahetsust ka selle üle, et kuigi mõiste „ajutiselt“ on esitatud korralduses mõnevõrra üksikasjalikumalt kui suunises PPD-28, tundub see andmekaitsenõukogu arvamuse kohaselt jätkuvalt tähendavat, et laiaulatuslik kogumine võib kesta seni, kuni objekti ei ole kindlaks määratud. Sellega seoses tuletab andmekaitsenõukogu meelde selgete ja täpsete eeskirjade vajalikkust ning juhib ka siinkohal tähelepanu, et need eeskirjad kujutavad endast andmesubjektide jaoks peamisi kaitsemeetmeid.

163. Kokkuvõttes tunneb andmekaitsenõukogu seoses andmete laiaulatusliku kogumise suhtes kohaldatavate eeskirjadega jätkuvalt muret selle pärast, et hoolimata korralduse EO 14086 alusel kehtestatud täiendavatest kaitsemeetmetest on endiselt ette nähtud võimalus koguda andmeid

[163] Euroopa Liidu Kohtu otsus Schrems II, punkt 183.
[164] Vt korraldus EO 14086, § 2(c)(ii)(D), ja otsuse eelnõu joonealune märkus nr 226.
[165] Lisaelemendid nende sätete kohta on esitatud eelmistes punktides.

laiaulatuslikult, see tähendab ilma kategooriateta, kusjuures kehtestatud ei ole selliseid peamisi kaitsemeetmeid nagu eelnev luba nende andmete kogumiseks (sealhulgas andmete ajutine tehniline laiaulatuslik kogumine erandolukorras), ning arvestades sealjuures ka vajadust täiendavate selgituste järele ja muret, mida on väljendatud seoses andmetele edasise juurdepääsu eesmärgi range piiramisega, andmete säilitamise selgete ja rangete eeskirjadega ning rangemate kaitsemeetmetega laiaulatuslikult kogutud andmete levitamise korral, sealhulgas edasisaatmise puhul.

164. Üldiselt rõhutab andmekaitsenõukogu, et eespool nimetatud Euroopa Inimõiguste Kohtu otsus näitab veel kord, kui tähtis on sõltumatute järelevalveasutuste tehtav põhjalik järelevalve. Andmekaitsenõukogu rõhutab, et sõltumatu järelevalve on riikliku julgeoleku eesmärgil toimuva valitsusepoolse andmetele juurdepääsu protsessi kõikides etappides oluline kaitsemeede meelevaldsete jälgimismeetmete vastu ja seega vajalik hindamaks, kas andmekaitse tase on piisav. Harta artikli 8 lõikes 3 osutatud järelevalveasutuste sõltumatuse tagatise eesmärk on tagada tõhus ja usaldusväärne järelevalve üksikisikute kaitse eeskirjade täitmise üle isikuandmete töötlemisel. See kehtib eelkõige olukordades, kus salajase jälgimise laadi tõttu ei ole üksikisikul võimalik taotleda läbivaatamist ega otseselt osaleda mis tahes läbivaatamismenetluses enne jälgimismeetme võtmist või selle ajal.

165. Andmekaitsenõukogu tuletab meelde, et tema arvamuse kohaselt sõltub kaitse piisavuse hinnang kõikidest juhtumi asjaoludest, eelkõige õigusraamistikuga ette nähtud hilisema järelevalve ja õiguskaitsevahendite tõhususest.

3.2.2.4 Õigusraamistik, millega on korraldatud andmete riikliku julgeoleku eesmärkidel toimuv konkreetne kogumine luureühenduse liikmete poolt USA territooriumil ja mujal

166. Kohtuotsuses Schrems II rõhutas Euroopa Liidu Kohus seoses FISA paragrahviga 702, et sellest tekstist „ei saa mingil viisil tuletada piiranguid selles ette nähtud volitusele rakendada jälgimisprogramme välisluureinfo saamiseks, nagu ka mitte kaitsemeetmeid USA-välistele isikutele, kes on nende programmide potentsiaalseks sihtmärgiks“[166]. Sellest tulenevalt leidis kohus, et „[n]eil asjaoludel [---] ei ole selle artikli abil võimalik tagada kaitse taset, mis oleks sisuliselt samaväärne hartaga tagatuga [---], mille kohaselt õiguslik alus, mis võimaldab põhiõiguste riivet, peab proportsionaalsuse põhimõttele vastamiseks ise määratlema, kui ulatuslikult tohib asjaomase õiguse teostamist piirata, ning nägema ette selged ja täpsed reeglid, mis reguleerivad asjaomase meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded“[167].

167. Seoses korraldusega EO 12333 märkis kohus, et see „ei anna õigusi, millele saaks USA ametiasutuste vastu kohtus tugineda“,[168] ning järeldas pärast nende tingimuste analüüsimist, mille alusel laiaulatuslik kogumine võib korralduse alusel koostoimes suunisega PPD-28 toimuda, ka seda, et „võimalus pääseda korraldusel E.O. 12333 põhinevate jälgimisprogrammide raames juurde USAsse liikuvatele andmetele, ilma et selle juurdepääsu suhtes toimuks mingitki kohtulikku kontrolli, ei sea igal juhul piisavalt selgelt ja täpselt piire isikuandmete sellisele laiaulatuslikule kogumisele“[169].

168. Nende konkreetsete andmekogumiskordade kohta on korralduses EO 14086 nüüd esitatud uued eeskirjad.

---

[166] Vt Euroopa Liidu Kohtu otsus Schrems II, punkt 180.
[167] Vt Euroopa Liidu Kohtu otsus Schrems II, punkt 180.
[168] Vt Euroopa Liidu Kohtu otsus Schrems II, punkt 182.
[169] Vt Euroopa Liidu Kohtu otsus Schrems II, punkt 183.

3.2.2.4.1 Riikliku julgeoleku eesmärgil andmete kogumine paragrahvi 702 alusel

169. Andmekaitsenõukogu tuletab meelde FISA paragrahvi 702 kohta tehtud järeldust,[170] mille kohaselt „praktikas saavad eri asutuste vähendamise ja/või eesmärgistatud kasutamisega seotud menetlustes ette nähtud juurdepääsu- ja säilitamispiirangutest kasu ka isikud väljastpoolt USAd, kuivõrd USA isikute teabe kindlakstegemise ja suurest andmekogumist eraldamise kulukuse ja keerukuse tõttu käsitletakse tavaliselt kogu andmekogumit kooskõlas kõige rangemate USA andmekaitsestandarditega".

170. Nende järelduste kohaselt „ei toimu programm teabevahetuse laiaulatusliku kogumise kaudu". Seda järeldust on kinnitatud ODNI avaldatud 2014. ja 2021. aasta statistilistes läbipaistvusaruannetes. Peale selle kasutatakse PCLOBi aruande andmeil jälgimise sihtmärgiks võtmiseks valikutingimusi, näiteks e-posti aadresse või telefoninumbreid.

171. Andmekaitsenõukogu tuletab aga meelde ka seda, et samal ajal selgitati andmekaitseraamistiku Privacy Shield viimases läbivaatamises seoses paragrahviga 702, et „isik", kes sihtmärgina kindlaks tehakse, võib osutada ka mitmele samu tunnuseid kasutavale üksikisikule, kui kõik need üksikisikud on USA-välised isikud ja vastavad samadele sihtmärgiks võtmise suhtes kohaldatavatele kriteeriumidele. Samuti tuletab andmekaitsenõukogu meelde, et andmekaitseraamistiku Privacy Shield kolmanda iga-aastase ühise läbivaatamise käigus 2019. aastal nõuti täiendavaid selgitusi seoses programmiga UPSTREAM, et välistada massiline ja valimatu juurdepääs USA-väliste isikute isikuandmetele[171].

172. Peale selle tuletab andmekaitsenõukogu meelde asjaolu, et FISA paragrahvi 702 alusel toimuvat andmete kogumist põhjendatakse sellega, et „kogumise oluliseks eesmärgiks on saada välisluureinfot", mis jätab teatava ebakindluse seoses selle eesmärgi piiramise ja vajalikkusega. Andmekaitsenõukogu märgib aga, et korralduse EO 14086 § 2(a)(A) ja (B) kohaselt tohib signaaliluurealast tegevust ellu viia üksnes pärast seda, kui on tehtud kindlaks, et see tegevus on vajalik kinnitatud prioriteedi edendamiseks, ning ainult sel määral ja sel viisil, mis on selle prioriteediga proportsionaalsed, ning et seda kohandatakse vastavalt sellele, mis on kinnitatud prioriteedi edendamiseks mõistlik, võttes nõuetekohaselt arvesse selliseid asjakohaseid tegureid nagu kogumisega kaasneva sekkumise ulatus, andmete tundlikkus ning ebaproportsionaalne mõju eraelu puutumatusele ja kodanikuvabadustele. Andmekaitsenõukogu ootab jätkuvalt täiendavaid selgitusi selle konkreetse rakendamise ja kasutuselevõtmise kohta, sealhulgas FISA paragrahvi 702 kohaldamise kontekstis.

173. Kuna andmekaitsenõukogul endal puudub otsene juurdepääs sellele teabele, kutsus ta üles koostama sõltumatut hinnangut FISA paragrahvi 702 kohase sihtmärkide määratluse ja mõiste „välisluure" vajalikkuse ja proportsionaalsuse kohta (sealhulgas programmi UPSTREAM raames) pärast selle paragrahvi ajakohastamist. Andmekaitsenõukogu leiab, et tema varasem nõue hinnata täiendavalt ja sõltumatult tunnuste konkreetsete juhtumite suhtes kohaldamise protsessi (tunnuste kindlaksmääramist) ning esitada lisaselgitusi seoses programmiga UPSTREAM on asjakohased. Uut korraldust EO 14086 arvesse võttes taotleb andmekaitsenõukogu seepärast lisateavet, et hinnata ja jälgida seda, kuidas ja mil määral hiljuti kehtestatud vajalikkuse ja proportsionaalsuse põhimõtteid selles kontekstis praktikas kohaldatakse, ning eeldab, et seda hinnatakse ka tulevaste ühiste läbivaatamiste käigus.

174. Andmekaitsenõukogu tunneb heameelt selle üle, et eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (Privacy and Civil Liberties Oversight Board – PCLOB) on sõltumatu järelevalveasutusena otsustanud korraldada „järelevalveprojekti, et uurida jälgimisprogrammi, mida

[170] Vt PCLOBi aruanne FISA paragrahvi 702 kohaselt rakendatava jälgimisprogrammi kohta, lk 100.
[171] Vt kolmanda ühise läbivaatamise aruanne, lk 17, punkt 83.

täitevvõim viib ellu välisluure ja jälitustegevuse seaduse (FISA) paragrahvi 702 kohaselt, arvestades paragrahvi 702 aegumistähtaega detsembris 2023 ning tulevast avalikku ja kongressis toimuvat arutelu selle uuesti lubamise kohta“[172]. Samuti tunneb andmekaitsenõukogu heameelt selle üle, et „läbivaatamine hõlmab valitud valdkondi, millele uurimine keskendub, sealhulgas, kuid mitte tingimata ainult, USA isikute päringuid paragrahvi 702 alusel kogutud teabe kohta ja programmi UPSTREAM raames paragrahvi 702 kohaselt kogutud andmete kogumist“[173] ning et „samuti hõlmab see programmi varasema ja prognoositud väärtuse ja tõhususe ning olemasolevate eraelu puutumatuse ja kodanikuvabaduste kaitsemeetmete piisavuse läbivaatamist“[174]. Sellest tulenevalt rõhutab andmekaitsenõukogu, et kõnealuse jälgimisprogrammi raames ette nähtud ja kohaldatavate eraelu puutumatuse kaitsemeetmete piisavaks ja igakülgseks hindamiseks on vaja juurdepääsu PCLOBi järeldustele selles paragrahvi 702 käsitlevas aruandes.

175. Võttes arvesse uut korraldust EO 14086, taotleb andmekaitsenõukogu täiendavalt lisateavet, et hinnata ja jälgida ka seda, kuidas ja mil määral hiljuti kehtestatud vajalikkuse ja proportsionaalsuse põhimõtteid ning muid nimetatud tekstis sätestatud kaitsemeetmeid selles kontekstis praktikas kohaldatakse.

3.2.2.4.2 Riikliku julgeoleku eesmärgil andmete kogumine korralduse 12333 alusel

176. Nagu Euroopa Liidu Kohus kohtuotsuses Schrems II tunnistas, ei tohiks nende kolmanda riigi õigusaktide analüüs, mille piisavust kaalutakse, piirduda õigusaktide ja tavadega, millega on lubatud jälgimistegevus asjaomase riigi füüsilistes piirides, vaid see peaks hõlmama ka analüüsi selles kolmandas riigis kehtivate õiguslike aluste kohta, mis võimaldavad tal viia läbi jälgimistegevust väljaspool oma territooriumi, sel määral, mil tegemist on ELi andmetega. Vajalikud piirangud seoses valitsuse juurdepääsuga andmetele peaksid laienema sellesse riiki „edastamisel olevatele“ isikuandmetele, mille pakutava kaitse piisavust tunnistatakse.

177. Andmekaitsenõukogu tunneb heameelt PCLOBi 2021. aasta aprillis avaldatud üldise avaliku aruande üle korralduse 12333 kohta, kuid märgib, et see aruanne jääb üldsõnaliseks, sest enamik järeldusi on salastatud.

178. Sellega seoses rõhutab andmekaitsenõukogu veel kord seda teksti käsitlevate PCLOBi oodatavate aruannete tähtsust, võttes arvesse ebakindlust ja ebaselgust seoses sellega, kuidas korraldust EO 12333 kohaldati, ning kuidas seda uut korraldust EO 14086 arvestades edaspidi kohaldatakse[175]. Andmekaitsenõukogu mõistab aga, et enamik nende sisust jääb salastatuks, seega ei tehta avalikkusele ega andmekaitsenõukogule kättesaadavaks täiendavat teavet korralduse EO 12333 täpse toimimise ning selle vajalikkuse ja proportsionaalsuse kohta.

179. Seepärast soovib andmekaitsenõukogu eelkõige, et PCLOBi aruannet korralduse EO 14086 kohaldamise kohta ei salastataks, vaid et see oleks pärast koostamist täielikult kättesaadav, sealhulgas need osad, milles hinnatakse korralduse EO 14086 kohaste kaitsemeetmete kohaldamist andmete

[172] Vt TEADE PCLOBI JÄRELEVALVEPROJEKTI KOHTA, MILLES UURITAKSE VÄLISLUURE JA JÄLITUSTEGEVUSE SEADUSE (FISA) PARAGRAHVI 702.

[173] Vt eespool.

[174] Vt eespool.

[175] Üldine aruanne korralduse EO 12333 kohta on enamjaolt jätkuvalt salastatud – avalikustatud on ainult lühike avalik versioon, samuti aruanne ja soovitused korralduse EO 12333 kohaselt läbiviidud Luure Keskagentuuri (CIA) terrorismivastase võitluse alase tegevuse kohta, mis on samuti vaid osaliselt avalik.

kogumise suhtes korralduse EO 12333 alusel. Samuti kutsub andmekaitsenõukogu komisjoni pöörama sellele küsimusele erilist tähelepanu tulevastes ühistes läbivaatamistes.

180. Üldiselt soovib andmekaitsenõukogu saada seoses USA õigusraamistikus sisalduvate eri õiguslike vahenditega, mis võimaldavad USA luureasutustel andmeid koguda ja neile edaspidi juurde pääseda ja neid töödelda, selgitusi nende koostoime kohta uue korraldusega EO 14086 ning eeldab kinnitusi selle kohta, et andmekaitsenõukogu varasemates arvamustes nende suhtes avaldatud varasemad kahtlused hajutatakse kõnealuste uute kaitsemeetmete vastuvõtmisega.

181. Samuti kutsub andmekaitsenõukogu komisjoni pöörama nendele aspektidele erilist tähelepanu tulevastes ühistes läbivaatamistes.

3.2.2.4.3 PCLOBi aruanne

182. Andmekaitsenõukogu tunneb heameelt selle üle, et korralduses EO 14086 on sätestatud ka nõue, mille kohaselt PCLOB peab koostama aruande korralduse rakendamise kohta. Andmekaitsenõukogu rõhutab, et see aruanne peaks sisaldama hinnangut korraldusega ette nähtud konkreetse võimaluse kohta koguda andmeid nii sihipärase kogumise puhul loetletud eesmärkidel kui ka laiaulatuslikult, sealhulgas tehnilistel põhjustel, et paremini mõista korralduses EO 14086 sätestatud põhitingimusi ning seda, kuidas neist praktikas aru saadakse ja kuidas neid eri jälgimisprogrammides kohaldatakse. See aruanne oleks vajalik ka selle hindamiseks, kuidas korraldust rakendatakse luureühenduse liikmete sisemenetlustes ja tegevuspõhimõtetes.

3.2.3 Tagatis C. Järelevalve

3.2.3.1 Sissejuhatus

183. USA luuretegevuse üle tehakse mitmetasandilist järelevalvet. USAs tehtava järelevalve ülesehituse saab jagada sisejärelevalveks ja väliseks järelevalveks. Kõigil luureühenduse liikmetel on järelevalve ja nõuetele vastavuse eest vastutavad ametnikud, kes teevad signaaliluurealase tegevuse üle korrapärast järelevalvet, sealhulgas eraelu puutumatuse ja kodanikuvabaduste ametnikud ja peainspektorid. Lisaks on olemas välised järelevalveorganid, nagu eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB) ning luuretegevuse järelevalve nõukogu (Intelligence Oversight Board).

184. Andmekaitsenõukogu tuletab meelde, et sekkumine leiab aset andmete kogumise ajal, aga ka ajal, mil avaliku sektori asutus neile andmetele edasise töötlemise eesmärgil juurde pääseb. Euroopa Inimõiguste Kohus on korduvalt täpsustanud, et mis tahes sekkumise suhtes eraelu puutumatuse ja andmekaitse õigusesse peab kehtima tõhus, sõltumatu ja erapooletu järelevalvesüsteem, mille on ette näinud kohtunik või mõni muu sõltumatu organ[176] (nt haldusasutus või parlamendiorgan).

185. Kuigi Euroopa Inimõiguste Kohus on väljendanud oma eelistust, et järelevalve tegemise eest vastutab kohtunik, ei välistanud ta võimalust, et vastutada võib ka mõni teine organ, „tingimusel et see asutus

[176] Kohtuotsus, Euroopa Inimõiguste Kohus, 6. september 1978, Klass ja teised *vs.* Saksamaa (edaspidi „Euroopa Inimõiguste Kohtu otsus Klass“), punktid 17 ja 51.

on piisavalt sõltumatu täitevvõimust“[177] ja „jälgimistegevust ellu viivatest asutustest ning [tal on] piisavad volitused ja pädevused tõhusa ja pideva kontrolli tegemiseks“[178].

186. Euroopa Inimõiguste Kohus lisas, et sõltumatuse hindamisel tuleb võtta arvesse „järelevalveorgani liikmete ametisse nimetamise viisi ja õiguslikku seisundit“[179].

187. Samuti märkis Euroopa Inimõiguste Kohus, et ta uurib, kas järelevalveorgani tegevust saab avalikult kontrollida. Seda võib teha näiteks seeläbi, et järelevalveorgan annab igal aastal aru valitsusele ning vastavad avalikud aruanded esitatakse parlamendile ja parlament arutab neid[180].

188. Euroopa Liidu Kohus võttis jälgimismeetmete rakendamise üle tehtavat sõltumatut järelevalvet arvesse ka kohtuotsuses Schrems II: „[---] FISC kontrolli eesmärk on kindlaks teha, kas need jälgimisprogrammid vastavad eesmärgile saada välisluureinfot, kuid ei puuduta küsimust, „kas isikud on välisluureinfo kogumise sihtmärgiks valitud õigesti““[181].

3.2.3.2 Sisejärelevalve

3.2.3.2.1 Peainspektorid

189. Andmekaitsenõukogu tunnistab, et peainspektoritele on antud luuretegevuse jälgimiseks vajalikud ulatuslikud volitused. Eelkõige on peainspektoritele kättesaadav kogu teave, mis on vajalik selleks, et hinnata asutuste töö üldist vastavust õigusaktidele, sealhulgas eraelu puutumatust ja andmekaitset käsitlevatele õigusaktidele, ning neil on õigus väljastada korraldusi ja võtta kõikidelt peainspektorite uurimistega seotud isikutelt vannet.

190. Eespool kirjeldatu põhjal leiab andmekaitsenõukogu, et üldiselt on peainspektoritel laialdased uurimisvolitused. Neil puuduvad aga siduvad volitused kaitsemeetmete kehtestamiseks ja nad annavad välja üksnes mittesiduvaid soovitusi[182].

191. Andmekaitsenõukogu tunnistab, et põhimõtteliselt ei takistata ega keelata peainspektoritel algatada, korraldada või viia lõpule mis tahes kontrolle või uurimisi ega anda kontrollide või uurimiste raames välja mis tahes korraldusi[183]. Andmekaitsenõukogu märgib aga sellega seoses, et peainspektorid tegutsevad vastava ministri alluvuses, ministri suuniste järgi ja tema kontrolli all; ministrid võivad keelata peainspektoritel teabele juurde pääseda, uurimist läbi viia ja muu hulgas anda välja mis tahes korraldusi juhul, kui minister leiab, et selline keeld on vajalik riikliku julgeoleku tagamiseks. Minister peab siiski teavitama selle volituse teostamisest USA kongressi vastutavaid komiteesid[184].

---

[177] Euroopa Inimõiguste Kohtu otsus Zakharov, punkt 258; kohtuotsus, Euroopa Inimõiguste Kohus, 10. veebruar 2009, Iordachi ja teised *vs.* Moldova, punktid 40 ja 51; kohtuotsus, Euroopa Inimõiguste Kohus, 26. aprill 2007, Dumitru Popescu *vs.* Rumeenia, punktid 70–73.

[178] Euroopa Inimõiguste Kohtu otsus Klass, punkt 56.

[179] Euroopa Inimõiguste Kohtu otsus Zakharov, punkt 278.

[180] Euroopa Inimõiguste Kohtu otsus Zakharov, punkt 283; Euroopa Inimõiguste Kohtu otsus, 9. juuni 1990, L. *vs.* Norra; Euroopa Inimõiguste Kohtu otsus, 18. mai 2010, Kennedy *vs.* Ühendkuningriik, punkt 166.

[181] Euroopa Liidu Kohtu otsus Schrems II, punkt 179.

[182] Otsuse eelnõu põhjendus 105.

[183] 1978. aasta peainspektori seadus (Inspector General Act of 1978), § 3 punkt a.

[184] Vt nt 1978. aasta peainspektori seadus, § 8 (kaitseministeeriumi kohta); § 8E (justiitsministeeriumi kohta), § 8G punkti d alapunkti 2 jaotised A ja B (Riikliku Julgeoleku Ameti (NSA) kohta); 50. U.S.C. § 403q punkt b (CIA kohta); 2010. eelarveaastaks vastu võetud luure volitamise seadus (Intelligence Authorization Act), § 405(f) (luureühenduse kohta).

192. Andmekaitsenõukogu märgib, et peainspektoreid saab ametist kõrvaldada ainult USA president, kes peab teavitama kongressi ametist kõrvaldamise põhjustest.

193. Andmekaitsenõukogu märgib, et sisejärelevalve mehhanismi ei ole alates artikli 29 töörühma ja seejärel andmekaitsenõukogu arvamuste vastuvõtmisest oluliselt muudetud. Seepärast järeldab andmekaitsenõukogu kooskõlas artikli 29 töörühma arvamusega 01/2016,[185] et üldiselt on kehtestatud piisavad sisejärelevalve mehhanismid.

3.2.3.3 Välisjärelevalve

194. Andmekaitsenõukogu märgib, et lisaks eespool nimetatud organitele teevad USA luureasutuste üle järelevalvet veel mitmesugused USA valitsuse organid, näiteks luuretegevuse järelevalve nõukogu ja kongressi komiteed. Viimati nimetatud võivad viia läbi oma uurimisi ja koostada aruandeid.

3.2.3.3.1 Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB)

195. Andmekaitsenõukogu tunnistab, et PCLOBil on seoses uue õiguskaitsemehhanismiga ja korralduse EO 14086 rakendamisega kõikehõlmav järelevalveroll.

196. Esiteks hõlmavad tema uued ülesanded justiitsministriga konsulteerimist seoses andmekaitse apellatsioonikohtu kohtunike ja erikaitsjate ametisse nimetamisega. Teiseks vaatab PCLOB igal aastal läbi õiguskaitse protsessi, see tähendab nõuetele vastavate kaebuste menetlemise õiguskaitsemehhanismi raames. See hõlmab küsimusi, kas CLPO ja andmekaitse apellatsioonikohus menetlesid nõuetele vastavaid kaebusi õigeaegselt, kas neil on täielik juurdepääs vajalikule teabele ja kas nad tegutsevad kooskõlas korraldusega EO 14086, samuti seda, kas luureühendus järgib CLPO ja andmekaitse apellatsioonikohtu otsuseid.

197. Peale selle tuleb PCLOBiga konsulteerida siis, kui luureasutused ajakohastavad oma sisemenetlusi ja tegevuspõhimõtteid korralduse EO 14086 rakendamiseks. Lisaks vaatab PCLOB ajakohastatud tegevuspõhimõtted ja menetlused läbi ning hindab nende vastavust korraldusele EO 14086[186]. Kuigi PCLOB järeldused ei ole rangelt võttes siduvad, on luureühenduse iga liikme juht kohustatud kõiki sellistes läbivaatamistes sisalduvaid soovitusi kooskõlas kohaldatavate õigusaktidega hoolikalt kaaluma ja rakendama või neid muul viisil käsitlema[187]. Kui otsuse eelnõu vastu võetakse, kutsub andmekaitsenõukogu komisjoni pöörama tulevastes läbivaatamistes erilist tähelepanu sellele, kas ja kuidas on PCLOBi soovitusi asutuste tasandil rakendatud.

198. Andmekaitsenõukogu tuletab meelde, et kuna PCLOB on sõltumatu, siis „õhutatakse“, mitte ei kohustata teda läbi vaatama, kas korralduses EO 14086 sisalduvaid kaitsemeetmeid on nõuetekohaselt arvesse võetud ja kas luureühendus on õiguskaitseprotsessi nõudeid täielikult järginud. Andmekaitsenõukogu saab aga olukorrast aru nii, et nagu PCLOB on andmekaitsenõukogule esitatud täiendavates selgitustes ja ka avalikult[188] märkinud, siis hakkab ta täitma korraldusega EO 14086 ette nähtud rolli.

199. Samuti tunneb andmekaitsenõukogu heameelt selle üle, et PCLOBi aruanded on kavas avalikkusele kättesaadavaks teha. Võttes arvesse asjaolu, et mitmesugused õiguskaitsemehhanismiga hõlmatud

[185] Artikli 29 töörühma arvamus 01/2016.
[186] Korraldus EO 14086, § 2(c)(iv) ja § 2(c)(v).
[187] Korraldus EO 14086, § 2(c)(v)(B).
[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

organid ja luureühenduse organid peavad PCLOBi aruannetes esitatud soovitusi põhimõtteliselt rakendama või neid muul viisil käsitlema, tunnistab andmekaitsenõukogu, et nendel soovitustel on eraelu puutumatuse kaitse meetmetes oluline roll.

200. Andmekaitsenõukogu märgib, et PCLOBi juurdepääs teabele on piiratud, kui USA president annab Ameerika Ühendriikide valitsuse ministeeriumidele, asutustele või üksustele[189] õiguse viia läbi „varjatud tegevust“[190].

201. Oma eelmiste arvamuste kohaselt leiab andmekaitsenõukogu, et PCLOB on sõltumatu organ, kelle soovitustel on olnud suur panus USAs tehtud reformidele ja kelle aruanded on olnud väga kasulik allikas mitmesuguste jälgimisprogrammide toimimise mõistmiseks, mis on järelevalvestruktuuri äärmiselt tähtis osa.

202. ELi-USA endise andmekaitseraamistiku Privacy Shield kolmandas iga-aastases ühises läbivaatamises avaldas andmekaitsenõukogu aga kahetsust, et PCLOB esitab andmekaitsenõukogule vaid sama teavet kui üldsusele. Samuti oli kahetsusväärne see, et PCLOB ei andnud välja täiendavaid aruandeid suunise PPD-28 kohta, et võtta järelmeetmeid oma esimese aruande suhtes eesmärgiga esitada lisaelemente selle kohta, kuidas PPD-28 kohaseid kaitsemeetmeid tuleb kohaldada, ega üldist ajakohastatud aruannet FISA paragrahvi 702 kohta.

203. Seepärast tunneb andmekaitsenõukogu heameelt selle üle, et PCLOB on andmekaitsenõukogu teavitanud FISA paragrahvi 702 käsitleva järelmeetmete aruande avaldamisest lähitulevikus. Lisaks on andmekaitsenõukogu rahul sellega, et PCLOB teavitas teda oma kohustusest avalikustada aruanded korralduse EO 14086 kohta. Andmekaitsenõukogu tuletab aga meelde, et salastamata aruannete avaldamine on reguleeritud USA õigusaktidega ja seda tuleb kooskõlastada luureühenduse asutustega – PCLOB ei saa selle kohta ise otsuseid teha.

204. Seepärast tuletab andmekaitsenõukogu meelde, et juhul, kui otsuse eelnõu vastu võetakse, peaks andmekaitsenõukogu julgeolekukontrolli läbinud ekspertidel olema võimalus kontrollida ELi-USA andmekaitseraamistiku tulevaste läbivaatamiste käigus vajaduse korral lisadokumente ja arutada täiendavat salastatud teavet eesmärgiga tagada, et aruannetes esitatud teavet on võimalik piisavalt hinnata, võttes samal ajal arvesse asjakohaseid riikliku julgeolekuga seotud huve ja eraelu puutumatuse suhtes kohaldatavat kaitset.

205. Andmekaitsenõukogu tunneb heameelt selle üle, et PCLOB on sõltumatu ja teeb järelevalvet riiklike luureasutuste üle, kes peavad PCLOBi soovitusi järgima või nendega muul viisil tegelema, mida käsitletakse PCLOBi aruandes USA kongressile.

206. Võttes arvesse Euroopa Inimõiguste Kohtu poolt seoses avaliku kontrolliga kehtestatud nõudeid,[191] mille kohaselt järelevalveorgani aruanded tuleb esitada parlamendile ja neid seal arutada, peab andmekaitsenõukogu piisavaks, et PCLOB esitab vähemalt kaks korda aastas aruande USA presidendile

[189] 42 U.S.C. § 2000ee punkti g alapunkt 5; 50 U.S.C. § 3093(a).
[190] Kooskõlas 50 U.S.C. § 3093(e) punktiga 1 tähendab termin „varjatud tegevus“ (*covert action*) Ameerika Ühendriikide valitsuse mis tahes tegevust või meetmeid välisriikides poliitiliste, majanduslike või sõjaliste tingimuste mõjutamiseks nii, et Ameerika Ühendriikide valitsuse roll ei ole ilmne ja seda avalikult ei tunnistata, kuid see ei hõlma 1) tegevust, mille põhieesmärk on hankida luureandmeid, traditsioonilist vastuluuretegevust.
[191] Euroopa Inimõiguste Kohtu otsus Zakharov, punkt 283; Euroopa Inimõiguste Kohtu otsus, 9. juuni 1990, L. *vs.* Norra; Euroopa Inimõiguste Kohtu otsus, 18. mai 2010, Kennedy *vs.* Ühendkuningriik, punkt 166.

ning eelkõige kongressi komiteedele senatis ja esindajatekojas,[192] s.o USA parlamentaarsetele organitele.

3.2.3.3.2 Vastuluurekohus (FISC)

207. Vastuluurekohus vastutab FISA paragrahvi 702 alusel toimuva isikuandmete kogumise üle tehtava järelevalve eest[193] ning FISC otsused saab edasi kaevata vastuluure apellatsioonikohtusse (Foreign Intelligence Surveillance Court of Review – FISCR).

208. FISC teeb järelevalvet FISA paragrahvi 702 alusel toimuva välisluureteabe kogumise sertifitseerimise protsessi üle ja annab loa elektroonilise teabe jälgimiseks, füüsiliseks läbiotsimiseks ja muudeks välisluure eesmärgil võetavateks uurimismeetmeteks[194]. Samuti annab FISC loa suunamis-, minimeerimis- ja sertifikaatide kohta päringute tegemise menetlusteks, mis on USA luureasutuste jaoks siduvad[195]. Kui FISC leiab, et nõudeid ei ole täidetud, võib ta sertifitseerimisest täielikult või osaliselt keelduda ning nõuda menetluste muutmist.

209. Kui tuvastatakse sihtmärgiks võtmise menetlusega seotud rikkumised, saab FISC nõuda asjaomaselt luureasutuselt parandusmeetmete võtmist[196]. Need parandusmeetmed ulatuvad individuaalsetest meetmetest struktuurimeetmeteni, näiteks andmete hankimise lõpetamisest ja ebaseaduslikult saadud andmete kustutamisest kuni kogumistavade, sealhulgas töötajatele antavate juhiste ja pakutava koolituse muutmiseni.

210. Andmekaitsenõukogu tunnistab, et korraldusega EO 14086 on ette nähtud, et CLPO ja andmekaitse apellatsioonikohus peavad teatama rikkumistest asejustiitsministrile riikliku julgeoleku küsimustes, kes teavitab nendest rikkumistest FISCd[197].

211. Nagu Euroopa Liidu Kohus kohtuotsuses Schrems II märkis, ei anna FISC luba üksikuteks jälgimismeetmeteks, vaid jälgimisprogrammideks[198]. Seepärast tunneb andmekaitsenõukogu jätkuvalt muret selle pärast, et FISC ei taga tõhusat kohtulikku järelevalvet USA-väliste isikute sihtmärgiks võtmise üle, ning tundub, et uue korraldusega EO 14086 ei ole seda küsimust lahendatud.

212. Mis puudutab FISA paragrahvi 702 kohast eelnevat sõltumatut jälgimistegevuse luba,[199] siis avaldab andmekaitsenõukogu kahetsust selle üle, et nagu tema otsuse eelnõust[200] ja USA valitsuse esitatud selgitustest aru saab, ei tundu FISC suhtes kehtivat korraldusega EO 14086 kehtestatud täiendavad kaitsemeetmed selliste programmide sertifitseerimise puhul, millega lubatakse võtta sihtmärgiks USA-väliseid isikuid. Andmekaitsenõukogu arvamuse kohaselt tuleks neid kõnealuses korralduses sisalduvaid täiendavaid kaitsemeetmeid sellises olukorras siiski arvesse võtta. Andmekaitsenõukogu tuletab meelde, et selle hindamisel, kuidas korralduse EO 14086 kohaseid kaitsemeetmeid

[192] 42 U.S.C. § 2000ee punkt e.
[193] 50 U.S.C. § 1881 punkt a.
[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court.
[195] 50 U.S.C. § 1881a punkt i.
[196] 50 U.S.C. § 1803 punkt h.
[197] Korraldus EO 14086, § 3(c)(i)(D); korraldus EO 14086, § 3(d)(i)(F).
[198] Euroopa Liidu Kohtu otsus Schrems II, punkt 179.
[199] Seoses andmete laiaulatusliku kogumisega korralduse EO 12333 alusel juhul, kui see ei kuulu FISC pädevusse, tunneb andmekaitsenõukogu muret selle pärast, et andmete laiaulatuslikuks kogumiseks ei ole kehtestatud eelneva loa saamise menetlust (vt ka tagatis B).
[200] Otsuse eelnõu põhjendus 165.

rakendatakse ning kuidas neid kaitsemeetmeid kohaldatakse juhul, kui andmeid kogutakse FISA paragrahvi 702 alusel, on väga kasulikud PCLOBi aruanded.

3.2.4 Tagatis D. Üksikisikule peavad olema kättesaadavad tõhusad õiguskaitsevahendid

213. Andmekaitsenõukogu tuletab meelde, et üksikisiku tõhusad ja kohtulikult kaitstavad õigused on äärmiselt olulised selle kindlakstegemisel, kas kolmandas riigis on andmekaitse piisav tase tagatud. Andmesubjektidel peab olema võimalus kasutada oma õiguste teostamiseks tõhusat õiguskaitsevahendit, kui nad leiavad, et neid õigusi ei austata või ei ole austatud. Euroopa Liidu Kohus on kohtuotsustes Schrems I ja II selgitanud, et „õigusakt, milles ei ole õigussubjektile ette nähtud mingit võimalust kasutada õiguskaitsevahendeid, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada, [ei järgi] harta artiklis 47 sätestatud põhiõiguse tõhusale kohtulikule kaitsele põhisisu“[201].

214. USA õiguskaitsevahendite süsteem sisaldab olulist piirangut, mille tõttu on väga keeruline algatada tavakohtus kohtumenetlust USA valitsuse võetud jälgimismeetmete vastu. USA põhiseaduse kohaselt peab üksikisik tõendama kaebeõigust, see tähendab „konkreetset, üksikasjalikku ja tegelikku või otsest kahju“[202]. Jälgimistegevusega seotud juhtudel tundub, et jälgitavate isikute teavitamata jätmine muudab selle nõude kehtetuks ka pärast seda, kui meetmed on lõppenud.

215. Sellega seoses tunneb andmekaitsenõukogu heameelt selle üle, et korralduses EO 14086 on kehtestatud konkreetne õiguskaitsemehhanism, et menetleda ja lahendada USA-väliste isikute kaebusi USA signaaliluurealase tegevuse kohta. Uue mehhanismi alusel kaebeõiguse nõuet ei kohaldata: korralduse EO 14086 § 4(k)(ii) kohaselt ei pea hageja tõendama, et tema andmete suhtes on läbi viidud USA signaaliluurealast tegevust. Seega saavad andmesubjektid tugineda korralduses EO 14086 kehtestatud kaitsemeetmetele, sealhulgas neile, mis on sätestatud korralduse 4. jao punkti d alapunktis iii ette nähtud muude asjakohaste õigusaktide ja sätetega[203]. Uus mehhanism lisab uue õiguskaitse saamise võimaluse, mis vastasel korral puuduks.

216. Uus mehhanism on kahetasandiline: esimese tasandi alusel saavad üksikisikud esitada kaebuse riikliku luurejuhi ameti kodanikuvabaduste kaitse ametnikule (CLPO). Teine tasand võimaldab üksikisikutel kaevata CLPO otsus edasi hiljuti loodud organisse, nn andmekaitse apellatsioonikohtusse (Data Protection Review Court – DPRC). Järgmistes punktides keskendutakse peamiselt õiguskaitsemehhanismi teisele tasandile. Andmekaitsenõukogu leiab, et valitsusametnikuna tegutsevale CLPO-le ei ole antud piisaval määral sõltumatust täitevvõimust ja seega ei saa ta ise piisavalt täita harta artiklist 47 tulenevaid nõudeid. Komisjon on seda hinnangut mitmel korral kinnitanud.

3.2.4.1 Kas andmekaitse apellatsioonikohtu loomine korralduse alusel on iseenesest piisav?

217. Andmekaitse apellatsioonikohus ei ole tavakohus, mille kongress on asutanud USA põhiseaduse III artikli alusel, vaid see põhineb USA presidendi välja antud korraldusel. Andmekaitsenõukogu on selle aluseks olevast põhimõttest – vältida kaebeõiguse tõendamise nõuet (vt ka punkt 215) – küll teadlik ja tunneb selle üle heameelt, kuid see tõstatab olulise küsimuse: kas selline õiguskaitsemehhanism

[201] Euroopa Liidu Kohtu otsus Schrems I, punkt 95; Euroopa Liidu Kohtu otsus Schrems II, punkt 187.
[202] Clapper *vs.* Amnesty International USA, 568 U.S. 398 (2013) II, lk 10.
[203] Korralduse EO 14086 §-ga 5(h) kehtestatakse sõnaselgelt andmesubjektide õigus esitada kooskõlas õiguskaitsemehhanismiga kaebusi.

vastab (üldse) harta artikli 47 nõuetele? Selle sätte kohaselt on igaühel, kelle liidu õigusega tagatud õigusi või vabadusi rikutakse, õigus tõhusale õiguskaitsevahendile seaduse alusel moodustatud kohtus.

218. Kui harta artikli 47 ingliskeelses sõnastuses on kasutatud väljendit „tribunal", siis ülejäänud keeleversioonides on eelistatud sõna „kohus"[204]. Euroopa Liidu Kohus kordas kohtuotsuses Schrems II, et andmesubjektil „peab olema võimalus kasutada õiguskaitsevahendeid sõltumatus ja erapooletus kohtus, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada"[205]. Samas andmekaitse taseme piisavuse hindamise kontekstis leiab aga Euroopa Liidu Kohus, et tõhusa õiguskaitse sellise sekkumise vastu saab tagada mitte üksnes kohus, vaid ka organ, mis pakub harta artiklis 47 nõututega sisuliselt samaväärseid tagatisi[206]. Samamoodi on Euroopa inimõiguste konventsioonis sätestatud, et „[i]gaühel, kelle [---] õigusi ja vabadusi on rikutud, on õigus tõhusale õiguskaitsevahendile riigivõimude ees",[207] mis, nagu Euroopa Inimõiguste Kohus on järjepidevalt sedastanud, ei pruugi tingimata olla õigusasutus[208]. Pigem on selle asutuse pakutava õiguskaitsevahendi tõhususe hindamisel asjakohased tema volitused ja menetluslikud tagatised, eeskätt see, kas ta on täitevvõimust sõltumatu ja tagab õiglase menetluse[209]. Tundub, et kumbki kohus ei lähtu oma hinnangus puhtvormilistest kriteeriumidest, vaid peavad määravaks sisulisi kaitsemeetmeid.

219. Kohtuotsuses Schrems II pööras Euroopa Liidu Kohus erilist tähelepanu tõhusale õiguskaitsevahendile riikliku julgeoleku eesmärgil isikuandmetele juurdepääsu valdkonnas. Andmekaitsenõukogu märgib, et sealjuures ei arutanud Euroopa Liidu Kohus harta artiklis 47 sisalduvat väljendit „seaduse alusel moodustatud", kuigi ka andmekaitseraamistiku Privacy Shield kohane ombusmani mehhanism ei põhinenud USA seadusel. Selle küsimuse käsitlemise asemel hindas Euroopa Liidu Kohus kaitse piisavuse kindlakstegemisel mitmesuguseid aspekte, näiteks volitusi kaitsemeetmete kehtestamiseks. Seega ei anta kohtuotsuses Schrems II mingeid suuniseid selle kohta, kuidas hinnata harta artikli 47 kohast mõistet „seaduse alusel moodustatud". Euroopa Liidu Kohus on seda küsimust aga kommenteerinud muudes kohtuotsustes. Kajastades Euroopa Inimõiguste Kohtu sellekohast kohtupraktikat, tuletas Euroopa Liidu Kohus kohtuasjades C-487/19 ja C-132/20 meelde, et termini „seaduse alusel moodustatud" eesmärk on tagada, et kohtusüsteemi korraldus demokraatlikus ühiskonnas ei jääks täitevvõimu meelevalda, vaid oleks reguleeritud seadusega, mille seadusandlik võim on vastu võtnud kooskõlas tema toimimist ja pädevust käsitlevate normidega[210]. Nagu sellest väitest ilmneb, on õigus pöörduda seaduse alusel moodustatud kohtusse väga tihedalt seotud sõltumatuse tagatisega.

220. Sellel taustal järeldab andmekaitsenõukogu, et kaitse taseme piisavuse hindamisel ei ole korralduse EO 14086 alusel loodud konkreetsed õiguskaitsemehhanismid erinevalt III artikli alusel moodustatud kohtute pakutavast õiguskaitsest iseenesest piisavad. Sellega seotud kaitsetaseme analüüs sõltub sellest, kas kaitsemeetmetega, mis on sätestatud korralduses EO 14086 ja mida täiendab

[204] Näiteks saksakeelses versioonis „Gericht".
[205] Euroopa Liidu Kohtu otsus Schrems II, punkt 194.
[206] Vt Euroopa Liidu Kohtu otsus Schrems II, punkt 197.
[207] Euroopa inimõiguste konventsiooni artikkel 13.
[208] Euroopa Inimõiguste Kohtu otsus Klass, punkt 67; Euroopa Inimõiguste Kohtu otsus Big Brother Watch, punkt 359.
[209] Euroopa Inimõiguste Kohtu otsus Klass, punkt 67; Euroopa Inimõiguste Kohtu otsus Big Brother Watch, punkt 359.
[210] Vt kohtuotsus, Euroopa Liidu Kohus, 6. oktoober 2021, W.Ż, C-487/19, ECLI:EU:C:2021:798, punkt 129, ja kohtuotsus, Euroopa Liidu Kohus, 29. märts 2022, Getin Noble Bank S.A., C-132/20, ECLI:EU:C:2022:235, punkt 121.

justiitsministri määrus, tagatakse piisavalt andmekaitse apellatsioonikohtu sõltumatus muudest võimudest.

221. Komisjon peaks pidevalt jälgima, kas korralduses EO 14086 ja seda täiendavates sätetes, eelkõige nendes sätetes, mille eesmärk on edendada andmekaitse apellatsiooninõukogu sõltumatust, kehtestatud eeskirju igakülgselt rakendatakse ja kas need toimivad praktikas tõhusalt. Peale selle tuleks hoolikalt läbi vaadata raamistiku mis tahes muudatuste mõju otsuse eelnõus esitatud komisjoni hinnangule. Sellega seoses märgib andmekaitsenõukogu, et korralduse EO 14086 ja justiitsministri määruse muutmise tagajärjel võidakse vastu võtta kohe kohaldatavad rakendusaktid, millega kaitse piisavuse otsus peatatakse, tühistatakse või seda muudetakse[211].

3.2.4.2 Piisav sõltumatus täitevvõimust

222. Kohtuotsuses Schrems II rõhutas Euroopa Liidu Kohus, et kõikide vajalike kaitsemeetmetega tuleb tagada kohtu või organi sõltumatus, eelkõige täitevvõimust, sealhulgas mis puudutab tagandamist või ametisse nimetamise tühistamist. Täpsemalt kritiseeris Euroopa Liidu Kohus asjaolu, et ombudsmani määras ametisse välisminister, kellele ta otseselt aru andis. Ombudsman kuulus USA välisministeeriumi koosseisu. Samuti leidis Euroopa Liidu Kohus, et seoses ombudsmani tagandamise või tema ametisse nimetamise tühistamisega puuduvad konkreetsed tagatised, mis kahjustab ombudsmani sõltumatust täitevvõimust.

223. Andmekaitsenõukogu tunnistab, et korralduse EO 14086 ja seda täiendava justiitsministri määruse sätetega ei kehtestata andmekaitse apellatsioonikohtule kohtustust justiitsministrile aru anda, nagu toimuks ülemuse-alluva suhte puhul. Samuti ei tee justiitsminister andmekaitse apellatsioonikohtu üle „igapäevast järelevalvet“[212]. Nende kaitsemeetmete näol on tegemist olulise edasiminekuga võrreldes andmekaitseraamistikuga Privacy Shield. Andmekaitse apellatsioonikohus on aga loodud täitevvõimu raames, nimelt justiitsministeeriumi haldusalas. Eeskätt sel põhjusel on kaitsemeetmete rakendamine ja tõhus toimimine praktikas äärmiselt olulised selle kindlakstegemiseks, kas andmekaitse apellatsioonikohut, mis ei ole küll justiitsministeeriumi lahutamatu osa, kuid kuulub siiski täitevvõimu alla, saab pidada tegelikkuses piisavalt sõltumatuks. Andmekaitsenõukogu kutsub komisjoni hoolikalt jälgima, kas need kaitsemeetmed praktikas täielikult kajastuvad. Lisaks soovitab andmekaitsenõukogu selgitada termini „igapäevane järelevalve“ puhul, et andmekaitse apellatsioonikohtu kohtunike üle ei tehta mingit järelevalvet. Komisjon on kinnitanud, et „igapäevast järelevalvet“ tuleb mõista selles tähenduses.

224. Võttes arvesse eespool kirjeldatud kaitsemeetmeid, nähakse ELi-USA andmekaitseraamistikuga ette teatavad tagatised seoses andmekaitse apellatsioonikohtu kohtunike ametisse nimetamise ja ametist tagandamisega. Kuigi kohtunikud nimetab ametisse justiitsminister, põhineb ametisse nimetamine kriteeriumidel, millest lähtutakse föderaalkohtunike kandidaatide hindamisel, ja see hõlmab konsulteerimist PCLOBiga. Kohtunikke saab enne nende ametiaja lõppu või pooleliolevast menetlusest tagandada ainult kitsalt määratletud asjaoludel, mis andmekaitsenõukogu arusaamise kohaselt on kujundatud föderaalkohtunike suhtes kohaldatavate sätete põhjal[213]. Nende eeskirjade kohaldamine on järgmine samm andmekaitse apellatsioonikohtu sõltumatu positsiooni tugevdamiseks, milleks samuti on äärmiselt oluline nende eeskirjade praktikas rakendamine. Otsuse eelnõust endast ei selgu aga, kas ja kuidas nende nõuete täitmist Ameerika Ühendriikides jälgitakse. Komisjoni ja USA valitsuse esitatud täiendavate selgituste põhjal saab andmekaitsenõukogu aru nii, et PCLOB võib käsitleda

[211] Otsuse eelnõu põhjendus 212.
[212] Justiitsministri määruse § 201.7 punkt d.
[213] Korraldus EO 14086, § 3(d)(iv); justiitsministri määruse § 201.7.

eespool nimetatud sätteid oma iga-aastases õiguskaitseprotsessi läbivaatamises ning et justiitsministeeriumi peainspektori kohustus kõikide õigusnõuete täitmist jälgida ja see tagada hõlmab korralduses EO 14086 ja andmekaitse apellatsioonikohtu asutamismäärustes sisalduvaid sätteid. Andmekaitsenõukogu kutsub komisjoni seda aspekti otsuse eelnõus selgitama. Lisaks peaks komisjon võtma neid kaitsemeetmeid arvesse, kui ta jälgib isikuandmete tegelikku töötlemist, mida otsuse eelnõus hinnatakse.

225. Otsuse eelnõus ei ole käsitletud küsimust, kas – ja kui, siis mis tingimustel – on USA presidendil õigus andmekaitse apellatsioonikohtu kohtunikke tagandada või ametist kõrvaldada. Andmekaitsenõukogu arusaamise kohaselt selline õigus puudub, nagu on selgitanud Euroopa Komisjon ja kinnitanud USA valitsuse esindajad. Andmekaitsenõukogu soovitab seda aspekti otsuse eelnõus selgitada.

226. Andmekaitse apellatsioonikohtu kohtunikud nimetatakse ametisse nelja-aastaseks ametiajaks ning algse ametisse nimetamise ajal ei tohi nad olla viimase kahe aasta jooksul töötanud täitevvõimu asutustes[214]. Andmekaitse apellatsioonikohtu kohtunike ametiaja jooksul ei tohi nad täita muid ametiülesandeid ega töötada USA valitsuses[215]. Erinevalt USA föderaalkohtunikest võivad nad aga tegeleda kohtuvälise tegevusega, muu hulgas äritegevuse, finantstegevuse, heategevusliku vahendite kogumise ja usaldusel põhineva tegevusega ning osutada õigusteenuseid, kui selline tegevus ei mõjuta erapooletust nende ametiülesannete täitmisel ega andmekaitse apellatsiooniohtu tulemuslikkust või sõltumatust[216]. Kohtunike sõltumatus ei seisne mitte üksnes selles, et nad ei võta vastu juhiseid, vaid ka isiklikus sõltumatuses. Siinkohal on asjakohased sellised tegurid nagu ametiaeg, võimalus saada uuesti ametisse nimetatud ja võimalikud huvide konfliktid. Korralduse EO 14086 ja vastavalt justiitsministri määruse alusel ette nähtud nelja-aastane ametiaeg on küll lühem kui Euroopa Liidu Kohtu kohtunike (kuus aastat koos uuesti ametisse nimetamise võimalusega) ja Euroopa Inimõiguste Kohtu kohtunike (üheksa aastat ilma uuesti ametisse nimetamise võimaluseta) ametiaeg, kuid see ei kujuta endast suurt probleemi. Andmekaitsenõukogu ei ole teadlik kohtupraktikast, millega kõnealune minimaalne ametiaeg kehtestatakse[217]. Samuti tunnistab andmekaitsenõukogu, et võimaluse suhtes tegeleda kohtuvälise tegevusega kehtib tingimus, mis lihtsalt väljendatuna seisneb selles, et selle tulemusel ei teki andmekaitse apellatsioonikohtu ülesandeid kahjustavat huvide konflikti. Andmekaitsenõukogu mõistab USA valitsuse täiendavate selgituste põhjal, et PCLOB ja justiitsministeeriumi peainspektor vaatavad ka need nõuded läbi ja teevad nende üle järelevalvet (vt punkt 226 ülalpool). Ühiste läbivaatamiste osana tuleks käsitleda ka seda, kuidas kõnealust nõuet praktikas kohaldatakse ja selle täitmist tõendatakse.

227. Korralduse EO 14086 § 3(d)(i)(B) kohaselt peab kõikidel andmekaitse apellatsioonikohtu kohtunikel olema juurdepääsuluba, et nad pääseksid juurde salastatud teabele, see tähendab, et neil oleks võimalik täita oma ülesannet langetada otsuseid riikliku julgeolekuga seotud kohtuasjades[218]. Mõne julgeolekukontrolli käsitleva Euroopa seaduse ja määrusega kohtunikud seevastu vabastatakse julgeolekukontrolli läbimise nõudest sel määral, mil nad täidavad kohtuniku ülesandeid, käsitades sellist üksikasjalikku kontrolli kohtuliku sõltumatusega potentsiaalselt vastuolus olevana[219]. USA valitsuse selgituse kohaselt läbib USA kohtusse kohtuniku ametikohale kandideerija küll põhjaliku

[214] Justiitsministri määruse § 201.3 punkt a.
[215] Justiitsministri määruse § 201.3 punkt c.
[216] Justiitsministri määruse § 201.7 punkt c.
[217] Vt muu hulgas kohtuotsus, Euroopa Inimõiguste Kohus (suurkoda), 25. mai 2021, Centrum För Rättvisa *vs.* Rootsi, punkt 346.
[218] Vt ka justiitsministri määruse § 201.11 punkt b ja otsuse eelnõu põhjendus 177.
[219] Nt Saksamaa julgeolekukontrolli seaduse § 2 lg 3.

kontrolli, kuid pärast USA kohtus föderaalkohtuniku ametisse nimetamist ei nõuta talt juurdepääsuloa saamist, et kohtuasjaga seotud salastatud dokumentidele juurde pääseda.

228. Andmekaitsenõukogu arvamuse kohaselt ilmnevad eespool kirjeldatud asjaoludest osalised erinevused USA föderaalkohtuniku ja andmekaitse apellatsioonikohtu kohtuniku ametikoha ja staatuse vahel. Tagatud kaitsemeetmed ei anna aga põhjust kahelda andmekaitse apellatsioonikohtu sõltumatuses. Kui otsuse eelnõu vastu võetakse, kutsub andmekaitsenõukogu tungivalt komisjoni käsitama eespool nimetatud kaitsemeetmeid ELi-USA andmekaitseraamistiku esimeses ühises läbivaatamises prioriteetsena. Andmekaitsenõukogu eeldab, et kui otsus vastu võetakse, täidab komisjon oma kohustust see peatada või kehtetuks tunnistada või seda muuta, kui USA täitevvõim otsustab korralduses sisalduvaid kaitsemeetmeid piirata[220].

3.2.4.3 Andmekaitse apellatsioonikohtu volitused

3.2.4.3.1 Juurdepääs teabele

229. Tõhusa õiguskaitse tagamiseks peavad kohtul olema piisavad uurimisvolitused vaidlustatud meetme läbivaatamiseks. Kohtuotsuses Kadi II sedastas Euroopa Liidu Kohus seoses harta artikliga 47, et Euroopa Liidu kohtud peavad tagama, et otsus põhineb arvestataval faktilisel alusel[221]. Euroopa Liidu Kohus märgib, et „liidu kohus [peab] alustama seda kontrolli, nõudes vajaduse korral liidu pädevalt asutuselt selle kontrolli jaoks asjakohaste konfidentsiaalsete või mittekonfidentsiaalsete andmete või tõendite esitamist“[222], kusjuures esitada ei saa „nende andmete või tõendite salastatuse või konfidentsiaalsuse vastuväidet“[223].

230. Otsuse eelnõu põhjenduse 181 kohaselt vaatab andmekaitse apellatsioonikohus CLPO otsused läbi, tuginedes vähemalt CLPO uurimise dokumentidele ning kaebuse esitaja, erikaitsja või luureasutuse esitatud mis tahes teabele ja materjalidele. Lisaks on otsuse eelnõus märgitud, et andmekaitse apellatsioonikohtul on juurdepääs kogu vajalikule teabele, mille ta võib saada CLPO kaudu. See põhineb justiitsministri määruse § 201.9 punktil b, millega andmekaitse apellatsioonikohtul lubatakse „nõuda, et ODNI CLPO täiendab dokumente konkreetse selgitava teabega ning teeb vajaduse korral täiendavaid faktilisi järeldusi, mis võimaldavad andmekaitse apellatsioonikohtu kolleegiumil läbivaatamine teostada“. Andmekaitsenõukogu arusaamise kohaselt ei ole andmekaitse apellatsioonikohtu tehtav hindamine seega mingil viisil piiratud järeldustega, mille CLPO tegi uue õiguskaitsemehhanismi esimesel tasandil. Vastupidi, andmekaitse apellatsioonikohus saab nõuda nii täiendava õigusliku teabe – ja mis veelgi olulisem – täiendavate faktiliste asjaolude esitamist, et analüüsida, kas toimunud on hõlmatud rikkumine. Samas märgib andmekaitsenõukogu ka seda, et need üldiselt laiaulatuslikud uurimisvolitused ei laiene juurdepääsule nendele andmetele, mida üksikisiku kohta hoitakse. Komisjon on selgitanud, et kui andmekaitse apellatsioonikohus nõuab lisateavet, tegutseb CLPO alati vahendajana. Seepärast sõltub andmekaitse apellatsioonikohtu juurdepääs teabele, mis on vajalik läbivaatamistaotluse kohta sõltumatu otsuse langetamiseks, teataval määral sellest, kas CLPO vajaliku teabe esitab. Andmekaitsenõukogu tunnistab, et CLPO-l on kohustus pakkuda andmekaitse apellatsioonikohtule „mis tahes vajalikku toetust“ ning luureasutused on kohustatud andma CLPO-le juurdepääsu andmekaitse apellatsioonikohtu läbivaatamiseks vajalikule

[220] Otsuse eelnõu põhjendus 212.
[221] Kohtuotsus, Euroopa Liidu Kohus, 18. juuli 2013, Euroopa Komisjon ja teised *vs.* Yassin Abdullah Kadi, C-584/10 P, C-593/10 P ja C-595/10 P (edaspidi „Euroopa Liidu Kohtu otsus Kadi II“), punkt 119.
[222] Euroopa Liidu Kohtu otsus Kadi II, punkt 120.
[223] Euroopa Liidu Kohtu otsus Kadi II, punkt 125.

teabele [224]. Andmekaitsenõukogu märgib aga ka seda, et CLPO ise ei ole sõltumatu ja viib läbi kaebuse esialgse uurimise õiguskaitsemenetluse esimeses etapis. Seepärast tunneb andmekaitsenõukogu heameelt selle üle, et PCLOB kontrollib õiguskaitsemehhanismi iga-aastase läbivaatamise käigus, kas andmekaitse apellatsioonikohus on saanud täieliku juurdepääsu kogu vajalikule teabele[225]. Peale selle kutsub andmekaitsenõukogu komisjoni juhul, kui otsuse eelnõu vastu võetakse, hõlmama seda aspekti ühistesse läbivaatamistesse, et uurida selle kehtiva süsteemi mõju.

3.2.4.3.2 Kaitsemeetmete kehtestamise volitused

231. Üks andmekaitseraamistiku Privacy Shield keskne puudus, mille tulemusel Euroopa Liidu Kohus raamistiku kohtuotsuses Schrems II kehtetuks tunnistas, olid ombudsmani ebapiisavad volitused kehtestada siduvaid kaitsemeetmeid. Euroopa Liidu Kohus leidis, et „ei ole [---] ühtki viidet sellele, et ombudsmanil on pädevus teha luureteenistustele siduvaid otsuseid“[226]. Üksnes USA valitsuse (poliitiline) kohustus, et luureühendus parandab kõik kohaldatavate eeskirjade rikkumised, mille ombudsman on avastanud, ei olnud piisav harta artikliga 47 tagatuga sisuliselt samaväärse kaitsetaseme tagamiseks.

232. Seevastu uue õiguskaitsemehhanismi alusel on CLPO ja andmekaitse apellatsioonikohtu otsustel siduv mõju[227]. Andmekaitsenõukogu tunnistab, et ühelt poolt ei piirdu need volitused konkreetsete meetmetega, vaid võimaldavad „asjakohaste kaitsemeetmete“ võtmist, et kindlakstehtud hõlmatud rikkumine „täielikult heastada“. Eelkõige on korralduse EO 14086 §-s 4(a) sõnaselgelt mainitud ebaseaduslikult kogutud andmete kustutamist. Teiselt poolt märgib andmekaitsenõukogu, et korralduse EO 14086 § 4(a) sõnastus tekitab teatavat ebakindlust seoses kõnealuste „asjakohaste kaitsemeetmete“ kindlaksmääramise protsessiga. Kuigi meede tuleks kavandada nii, et see rikkumise täielikult heastaks, tuleb kaaluda ka „viise, kuidas seda laadi rikkumisi, nagu kindlaks tehti, on tavaliselt käsitletud“[228]. Selle nõude tähendus ja mõju on ebaselged. Seepärast kutsub andmekaitsenõukogu komisjoni hoolikalt jälgima vastuvõetud kaitsemeetmete toimimist praktikas.

3.2.4.4 Kaebuse esitamine uue õiguskaitsemehhanismi alusel

233. Korralduse EO 14086 alusel loodud õiguskaitsemehhanismi kohaldatakse ainult nõuetele vastavate kaebuste suhtes, mille esitab nõuetele vastava riigi asjakohane avaliku sektori asutus Ameerika Ühendriikide signaaliluurealase tegevusega seotud mis tahes hõlmatud rikkumise kohta[229]. Seega peavad selle õiguskaitsevahendi kasutamiseks olema täidetud mitu tingimust.

3.2.4.4.1 Nõuetele vastavaks riigiks nimetamine

234. Esiteks peab riik või piirkondliku majandusintegratsiooni organisatsioon, kust andmed Ameerika Ühendriikidesse edastati, olema enne kaebuse aluseks olevat andmeedastust nimetatud nõuetele vastavaks riigiks[230]. Ilmselgelt on väga oluline, et ajal, mil kaitse piisavuse otsus jõustub, on ettenähtud õiguskaitsemehhanism kasutatav. Sellest tulenevalt on otsuse eelnõu põhjenduses 196 sätestatud, et otsuse jõustumine sõltub muu hulgas sellest, kas liit on õiguskaitsemehhanismi kohaldamise eesmärgil nimetatud nõuetele vastavaks üksuseks. Tegelikult näib komisjon eeldavat, et nimetamine toimub

[224] Korraldus EO 14086, § 3(c)(i)(H) ja § 3(d)(iii).
[225] Korraldus EO 14086, § 3(e)(i).
[226] Euroopa Liidu Kohtu otsus Schrems II, punkt 196.
[227] Vastavalt korralduse EO 14086 § 3(c)(ii) ja § 3(d)(ii).
[228] Korraldus EO 14086, § 4(a).
[229] Korraldus EO 14086, § 3(a).
[230] Korraldus EO 14086, § 4(d)(i) ja § 4(k)(i).

enne otsuse vastuvõtmist, sest eelnõu juba sisaldab täitmata kohta ELi nõuetele vastavaks riigiks nimetamise jaoks justiitsministri poolt[231] (selle asemel et lisada nimetamine kui eeltingimus otsuse eelnõu resolutiivossa).

3.2.4.4.2 Kahjulik mõju eraelu puutumatusele ja kodanikuvabadustele ning kaebeõigus

235. Nõuetele vastav kaebus peab põhinema väidetaval hõlmatud rikkumisel, mis omakorda tähendab seda, et rikkumine peab kahjulikult mõjutama kaebuse esitaja eraelu puutumatuse ja kodanikuvabadustega seotud huve[232]. Komisjoni lisaselgituste põhjal saab andmekaitsenõukogu sellest aru nii, et kahjulik mõjutamine ei tähenda kaebuse vastuvõetavuse mingis vormis piiramist. Nagu komisjon väitis, on selline kahjulik mõju pigem seotud mis tahes kaebustega, mis käsitlevad signaaliluurealase tegevuse raames isikuandmete töötlemist, millega rikutakse korralduse EO 14086 §- s 4(d)(iii) osutatud sätteid, näiteks korralduses kehtestatud kaitsemeetmeid. Andmekaitsenõukogu väljendab kahetsust selle üle, et seda ei ole otsuse eelnõus täpsustatud, ja kutsub komisjoni täiendavalt selgitama „kahjuliku mõju“ mõistet, et tagada andmesubjektide mis tahes õiguse rikkumise hindamine ja heastamine ning see, et õiguskaitse ja asjakohaste kaitsemeetmete kasutamiseks ei tule tõendada mingit raskusastet.

236. Nagu juba mainitud, ei pea kaebuse esitaja korralduse EO 14086 alusel kaebuse esitamisel tõendama kaebeõigust (vt punkt 215)[233]. Andmekaitsenõukogu tunneb heameelt korralduse EO 14086 §-s 4(k) esitatud selgituse üle, mille kohaselt lähtutakse arvamusest, ning seda, et kaebuse esitaja andmetele on signaaliluurealase tegevuse kaudu tegelikult juurde pääsetud, ei ole vaja tõendada. Õiguskaitsemehhanismi loomine on oluline samm, sest kaebeõiguse nõude tõttu on väga keeruline jälgimismeetmeid Ameerika Ühendriikide tavakohtutes vaidlustada.

237. Eespool kirjeldatu põhjal ei leia andmekaitsenõukogu, et tavakohtusse pöördumine, millele otsuse eelnõus on samuti viidatud,[234] pakub piisavat kaitsetaset[235]. Sellega seoses tuletab andmekaitsenõukogu meelde, et ta on juba korduvalt väljendanud muret seoses tavakohtute puhul kehtiva kaebeõiguse nõudega[236]. Peale selle saab andmekaitsenõukogu USA valitsuse täiendavate selgituste põhjal aru nii, et kuigi EO 14086 ei välista üldise pädevusega kohtusse pöördumist, siis ei ole kindel, kuidas selline kohus kõnealust korraldust kohaldaks. Kui otsuse eelnõu vastu võetakse, võiks seda küsimust tulevastes läbivaatamistes täiendavalt uurida.

3.2.4.4.3 Kaebuse menetlemine

238. Andmekaitsenõukogu kiidab põhimõtteliselt heaks menetluse, mille kohaselt kaebus esitatakse liikmesriikide järelevalveasutuste kaudu, ning on jätkuvalt arvamusel, et kaebuse esitaja isikusamasust tuleks kontrollida ELi territooriumil. Ent sarnaselt andmekaitseraamistiku Privacy Shield kohase ombudsmani mehhanismiga on otsuse eelnõus sätestatud, et andmesubjekt, kes soovib sellist kaebust esitada, peab selle esitama ELi liikmesriigi järelevalveasutusele, kes on pädev tegema järelevalvet riiklike julgeolekuteenistuste üle ja/või isikuandmete töötlemise üle avaliku sektori asutuste poolt[237]. Sellega seoses tuletab andmekaitsenõukogu meelde murekohti, mille ta juba tõstatas artikli 29

[231] Otsuse eelnõu põhjendus 320.
[232] Korraldus EO 14086, § 4(k)(i) ja § 4(d)(ii).
[233] Clapper *vs.* Amnesty International USA, 568 U.S. 398 (2013) II, lk 10.
[234] Otsuse eelnõu põhjendus 187 jj.
[235] Vt ka Euroopa Liidu Kohtu otsus Schrems II, punktid 191 ja 192.
[236] Vt artikli 29 töörühma arvamus 01/2016, lk 43.
[237] Otsuse eelnõu põhjendus 169.

töörühma arvamuses andmekaitseraamistiku Privacy Shield kohta, näiteks üksikisikute võimalikke probleeme pädeva asutuse kindlakstegemisel, arvestades liikmesriikide julgeolekuteenistuste järelevalvemehhanismide mitmekesisust[238]. Võttes arvesse riiklike andmekaitseasutuste kaasamist ELi-USA andmekaitseraamistiku kohaldamisse ja selle üle tehtavasse järelevalvesse, on asjakohasem esitada kaebusi nende kaudu.

3.2.4.5 Andmekaitse apellatsioonikohtu otsus

239. Pärast kaebuse esitaja taotluse läbivaatamist ei tohi andmekaitse apellatsioonikohus avalikustada, kas kaebuse esitaja suhtes viidi läbi USA signaaliluurealast tegevust. Selle asemel teavitatakse kaebuse esitajat, et „läbivaatamise käigus ei tuvastatud mingeid hõlmatud rikkumisi või tegi andmekaitse apellatsioonikohus otsuse, millega nõutakse asjakohaste kaitsemeetmete võtmist“[239]. Selle standardvastuse üldine seadusjärgne eesmärk on kaitsta tundlikku teavet USA luuretegevuse kohta. Andmekaitsenõukogu tunneb aga muret selle pärast, et korraldusega EO 14086 ei ole ette nähtud mingeid erandeid andmekaitse apellatsioonikohtu standardvastusest.

240. Kohtuasjas Kadi II pidi Euroopa Liidu Kohus käsitlema vastandlikke huve ühelt poolt riigisaladuse hoidmise ning teiselt poolt ausa ja võimalikult suures ulatuses võistleva kohtumenetluse vahel. Euroopa Liidu Kohus sedastas, et olukorras, kus riikliku julgeolekuga seotud ülekaalukad kaalutlused takistavad asjaomasele isikule teatud andmetest või tõenditest teatamist, on kohtu ülesanne siiski kohaldada kohtuliku kontrolli raames vahendeid, mis võimaldavad tasakaalustada legitiimseid julgeolekukaalutlusi ja vajadust tagada piisavas ulatuses üksikisiku menetlusõiguste kaitse, nagu õigus olla ära kuulatud ja võistlevuse põhimõte[240]. Lisaks täpsustas Euroopa Liidu Kohus, et kohus peab liidu pädeva asutuse esitatud õiguslikke ja faktilisi asjaolusid kogumis analüüsides kontrollima, kas nimetatud asutuse esitatud põhjendused selle kohta, miks selline teatamine ei ole võimalik, on põhjendatud[241]. Kui ilmneb, et liidu pädeva asutuse viidatud põhjused ei võimalda tegelikult teavitada asjaomast isikut andmetest ja tõenditest, siis tuleb siiski viia nõuded, mis on seotud õigusega tõhusale kohtulikule kontrollile, sobival viisil tasakaalu nõuetega, mis tulenevad riiklikust julgeolekust[242]. Niisuguse tasakaalustamise eesmärgil on lubatud kasutada selliseid võimalusi nagu asjassepuutuva teabe või tõendite sisu kokkuvõtte teatavakstegemine[243]. Kuigi Euroopa Liidu Kohtu järeldustega ei kehtestata nõudeid kohtu otsuse kohta, vaid pigem käsitlevad need pädeva asutuse otsust ja kohtumenetluse läbiviimist, annavad need teavet eespool nimetatud huvide tasakaalu viimise kohta seoses õigusega tõhusale õiguskaitsele. Täiendavate suuniste saamiseks võib tutvuda ka kohtuotsusega Big Brother Watch, kus Euroopa Inimõiguste Kohus sedastas menetluse õiglusele ja eeskätt võistlevale kohtumenetlusele osutades, et kohtu või muu sõltumatu organi otsused peavad olema põhjendatud[244].

241. Andmekaitsenõukogu tunnistab, et andmekaitse apellatsioonikohtu otsused on tõepoolest põhjendatud. Andmekaitse apellatsioonikohus on sõnaselgelt kohustatud tegema kirjaliku otsuse, milles on kirjeldatud tema analüüsi ja täpsustatud võimalikke asjakohaseid kaitsemeetmeid[245]. Lisaks märgib andmekaitsenõukogu, et üksikisikut teavitatakse, kui andmekaitse apellatsioonikohtu

[238] Artikli 29 töörühma arvamus 01/2016, lk 48–49.
[239] Korraldus EO 14086, § 3(d)(i)(H). Korraldusega EO 14086 on selline vastus ette nähtud ka CLPO puhul.
[240] Euroopa Liidu Kohtu otsus Kadi II, punkt 125.
[241] Euroopa Liidu Kohtu otsus Kadi II, punkt 126.
[242] Euroopa Liidu Kohtu otsus Kadi II, punkt 128.
[243] Euroopa Liidu Kohtu otsus Kadi II, punkt 129.
[244] Euroopa Inimõiguste Kohtu otsus Big Brother Watch, punkt 359.
[245] Justiitsministri määruse § 201.9 punkt g.

läbivaatamisega hõlmatud teabe salastatus kustutatakse[246]. Samuti tunnustab andmekaitsenõukogu uue õiguskaitsemehhanismiga ette nähtud erikaitsjate rolli, mis hõlmab kaebuse esitaja huvide eest seismist asjaomases küsimuses[247]. Võttes aga arvesse Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu eespool kirjeldatud kohtupraktika mõju ja asjaolu, et andmekaitse apellatsioonikohtu otsust ei saa edasi kaevata, vaid see on lõplik,[248] tunneb andmekaitsenõukogu muret andmekaitse apellatsioonikohtu standardvastuse üldise kohaldatavuse pärast. Andmekaitsenõukogu tuletab meelde, et PCLOB vaatab uue õiguskaitsemehhanismi toimimise sõltumatult läbi, ja kutsub komisjoni juhul, kui otsus vastu võetakse, pöörama tulevastes läbivaatamistes sellele küsimusele, sealhulgas PCLOB võimalikele hinnangutele selle aspekti kohta, erilist tähelepanu.

4 OTSUSE EELNÕU RAKENDAMINE JA JÄLGIMINE

242. Seoses otsuse eelnõu jälgimise ja läbivaatamisega märgib andmekaitsenõukogu, et Euroopa Liidu Kohtu praktikas on sätestatud järgmine: „[K]una kolmanda riigi tagatav kaitsetase võib muutuda, peab komisjon pärast [isikuandmete kaitse üldmääruse artikli 45] alusel otsuse tegemist regulaarselt kontrollima, kas järeldus kõnealuse kolmanda riigi tagatava kaitse piisava taseme kohta on jätkuvalt faktiliselt ja õiguslikult põhjendatud. Niisugune kontrollimine on igal juhul nõutav, kui teatud asjaolud tekitavad vastava kahtluse“[249].

243. Peale selle märgib andmekaitsenõukogu, et kaubandusministeeriumi kirjas on mainitud, et kaubandusministeerium ja vajaduse korral teised USA asutused korraldavad komisjoni, ELi huvitatud andmekaitseasutuste ja andmekaitsenõukogu asjakohaste esindajatega korrapäraseid koosolekuid[250].

244. Andmekaitsenõukogu leiab, et järgmiste korrapäraste läbivaatamiste käigus tuleks pöörata erilist tähelepanu osariigi õigusega antavale kaitsele seoses õiguskaitseasutuste juurdepääsuga, USA riikliku julgeolekuasutuste poolset ajutist laiaulatuslikku kogumist käsitlevale erandile sihipärase kogumise eesmärgil, hiljuti kehtestatud vajalikkuse ja proportsionaalsuse põhimõtete praktikas kohaldamisele, sealhulgas programmi UPSTREAM raames, korralduse EO 14086 ja selliste USA mitmesuguste õigusaktide koostoimele, millega lubatakse USA luureasutustel isikuandmeid koguda ja täiendavalt töödelda, sellistele sisemenetlustele ja tegevuspõhimõtetele, millega raamistikku rakendatakse, sellele, kuidas neid kaitsemeetmeid võetakse arvesse ka FISC juhtimisel toimuvas järelevalves ning kuidas õiguskaitsemehhanism tõhusalt toimib, ning edasisaatmise küsimusele, automaatsel töötlemisel põhinevatele otsustele, andmekaitseraamistiku põhimõtete sisulisele ja tõhusale järelevalvele ja täitmise tagamisele, samuti tõhusale õiguskaitsevahendile.

245. Andmekaitsenõukogu märgib, et kaitse piisavuse otsus vaadatakse läbi ühe aasta jooksul pärast liikmesriikidele kaitse piisavuse otsusest teatamist ning seejärel vähemalt iga nelja aasta tagant[251]. Selleks et kaitse piisavuse otsuse pidevat jälgimist veelgi tugevdada, kutsub andmekaitsenõukogu komisjoni tegema järgnevaid läbivaatamisi vähemalt iga kolme aasta tagant.

246. Mis puudutab andmekaitsenõukogu ja tema esindajate praktilist kaasamist tulevaste korrapäraste läbivaatamiste ettevalmistamisse ja läbiviimisse, siis kordab andmekaitsenõukogu, et temaga tuleks piisavalt varakult enne läbivaatamist kirjalikult jagada kõiki asjakohaseid dokumente, sealhulgas

[246] Korraldus EO 14086, § 3(d)(v).
[247] Justiitsministri määruse § 201.8 punkt g.
[248] Justiitsministri määruse § 201.9 punkt g.
[249] Euroopa Liidu Kohtu otsus Schrems I, punkt 76. Vt ka otsuse eelnõu artikli 3 lõige 4.
[250] Otsuse eelnõu III lisa.
[251] Otsuse eelnõu artikli 3 lõige 4.

kirjavahetust. Sarnaselt andmekaitseraamistiku Privacy Shield alusel tehtud läbivaatamistega soovitab andmekaitsenõukogu vähemalt kolm kuud enne läbivaatamist määrata kindlaks läbivaatamise üksikasjad ning nendes komisjoni, USA valitsuse ja andmekaitsenõukogu vahel kokku leppida.

247. Peale selle märgib andmekaitsenõukogu ära ja tunneb heameelt selle üle, et otsuse eelnõu põhjenduses 212 on esitatud näiteid muudatustest, mis võivad kaitse taset kahjustada ning mille korral võib olla põhjendatud nn erakorralise kehtetuks tunnistamise menetluse algatamine, milles keskendutakse sellistele muudatustele, mida võidakse teha seoses korraldusega EO 14086 ja seotud justiitsministri määrusega.

Euroopa Andmekaitsenõukogu nimel

eesistuja

(Andrea Jelinek)